



## **Cisco IP Conference Phone 8832 Multiplatform Phones Administration Guide for Release 11.3(1) and Later**

**First Published:** 2019-11-19

**Last Modified:** 2022-06-28

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022 Cisco Systems, Inc. All rights reserved.



## CONTENTS

---

### CHAPTER 1

<b>Cisco IP Conference Phone Hardware</b>	<b>1</b>
Cisco IP Conference Phone 8832	1
Phones Supported in this Document	3
Cisco IP Conference Phone 8832 Buttons and Hardware	3
Conference Phone Softkeys	4
Wired Expansion Microphone	4
Wireless Expansion Microphone	5
Cisco IP Conference Phone 8832 Documentation	6
Terminology Differences	6

---

### CHAPTER 2

<b>New and Changed Information</b>	<b>7</b>
New and Changed for Firmware Release 11.3(7)	7
New and Changed for Firmware Release 11.3(6)	8
New and Changed for Firmware Release 11.3(5)	9
New and Changed for Firmware Release 11.3(4)	10
New and Changed for Firmware Release 11.3(3)	10
New and Changed for Firmware Release 11.3(2)	11
New and Changed for Firmware Release 11.3(1)	13
New and Changed for Firmware Release 11.2(3)SR1	14

---

### PART I

<b>Cisco IP Phone Provisioning</b>	<b>15</b>
------------------------------------	-----------

---

### CHAPTER 3

<b>Provisioning</b>	<b>17</b>
Provisioning Overview	17
Provisioning	18
Normal Provisioning Server	19

Phone Provisioning Practices	19
Onboard Your Phone with the Activation Code	19
Phone Onboarding to Webex Cloud	20
Enable a Phone to Onboarding to Webex Cloud	20
Enable Auto Provisioning with Short Activation Code	20
Manually Provision a Phone from the Keypad	21
DNS SRV for HTTP Provisioning	22
Use DNS SRV for HTTP Provisioning	23
Set the Profile Rule with the SRV Option on the Web Page	24
Set the Profile Rule with the SRV Option on the Phone	24
TR69 Provisioning	25
TR69 RPC Methods	25
RPC Methods Supported	25
Event Types Supported	26
Communication Encryption	26
Phone Behavior During Times of Network Congestion	26
In-House Preprovisioning and Provisioning Servers	26
Server Preparation and Software Tools	27
Remote Customization (RC) Distribution	28
In-House Device Preprovisioning	29
Provisioning Server Setup	29
TFTP Provisioning	30
Remote Endpoint Control and NAT	30
HTTP Provisioning	30
HTTP Status Code Handling on Resync and Upgrade	31

**CHAPTER 4****Provisioning Methods 33**

Provision a Phone with BroadSoft Server	33
Provisioning Examples Overview	34
Basic Resync	34
Use Syslog to Log Messages	34
TFTP Resync	34
Log Messages to the Syslog Server	35
System Log Parameters	36

Unique Profiles, Macro Expansion, and HTTP	38
Provision a Specific IP Phone Profile on a TFTP Server	38
HTTP GET Resync	38
Resync with HTTP GET	39
Provisioning Through Cisco XML	39
URL Resolution with Macro Expansion	40
Resync a Device Automatically	40
Profile Resync Parameters	41
Set Up Your Phones for Activation Code Onboarding	48
Activation Code Provisioning Parameters	48
Migrate Your Phone to Enterprise Phone Directly	49
Secure HTTPS Resync	50
Basic HTTPS Resync	50
Authenticate with Basic HTTPS Resync	51
HTTPS with Client Certificate Authentication	52
Authenticate HTTPS with Client Certificate	52
Configure a HTTPS Server for Client Filtering and Dynamic Content	53
HTTPS Certificates	54
HTTPS Methodology	54
SSL Server Certificate	54
Obtain a Server Certificate	55
Client Certificate	55
Certificate Structure	55
Configure a Custom Certificate Authority	56
Profile Management	57
Compress an Open Profile with Gzip	57
Encrypt a Profile with OpenSSL	58
Create Partitioned Profiles	59
Set the Phone Privacy Header	59
Renew the MIC Certificate	60
Parameters for MIC Certificate Renewal by SUDI Service	61

---

**CHAPTER 5**
**Provisioning Parameters 63**

Provisioning Parameters Overview	63
----------------------------------	----

- Configuration Profile Parameters 63
- Firmware Upgrade Parameters 68
- General Purpose Parameters 69
- Macro Expansion Variables 69
- Internal Error Codes 72

---

**CHAPTER 6**

**Provisioning Formats 73**

- Configuration Profiles 73
- Configuration Profile Formats 73
  - Configuration File Components 74
    - Element Tag Properties 74
    - Parameter Properties 76
    - String Formats 76
- Open Profile (XML) Compression and Encryption 77
  - Open Profile Compression 77
  - Open Profile Encryption 77
    - AES-256-CBC Encryption 78
    - RFC 8188-Based HTTP Content Encryption 81
  - Optional Resync Arguments 82
    - key 82
    - uid and pwd 82
- Application of a Profile to the Phone 83
  - Download the Configuration File to the Phone from a TFTP Server 83
  - Download the Configuration File to the Phone with cURL 83
- Provisioning Parameter Types 84
  - General Purpose Parameters 84
    - Use General Purpose Parameters 85
  - Enable Parameters 85
  - Triggers 85
    - Resync at Specific Intervals 86
    - Resync at a Specific Time 86
  - Configurable Schedules 86
  - Profile Rules 87
  - Upgrade Rule 89

Data Types	90
Profile Updates and Firmware Upgrades	93
Allow Profile Updates	93
Allow and Configure Firmware Upgrades	94
Upgrade Firmware by TFTP, HTTP, or HTTPS	95
Upgrade Firmware With a Browser Command	95

---

**PART II****Cisco IP Phone Configuration 97**

---

**CHAPTER 7****Access Control Configuration 99**

Access Control	99
Administrator and User Accounts	99
User Access Attribute	100
Access the Phone Web Interface	100
Control Access to the Phone Settings	101
Access Control Parameters	101
Bypass the Set Password Screen	104

---

**CHAPTER 8****Third-Party Call Control Setup 105**

Determine the Phone MAC Address	105
Network Configuration	105
Provisioning	106
Report Current Phone Configuration to the Provisioning Server	106
Parameters for Reporting the Phone Configuration to the Server	109

---

**CHAPTER 9****Cisco IP Phone Security 113**

Domain and Internet Setting	113
Configure Restricted Access Domains	113
Configure the DHCP Options	114
Parameters for DHCP Options Configuration	114
DHCP Option Support	115
Configure the Challenge for SIP INVITE Messages	116
Transport Layer Security	117
Encrypt Signaling with SIP Over TLS	117

Configure LDAP over TLS	118
Configure StartTLS	118
HTTPS Provisioning	119
Get a Signed Server Certificate	120
Multiplatform Phone CA Client Root Certificate	121
Redundant Provisioning Servers	121
Syslog Server	122
Enable the Firewall	122
Configure Your Firewall with Additional Options	123
Configure the Cipher List	125
Supported Cipher Strings	127
Enable Hostname Verification for SIP over TLS	128
Enable Client-Initiated Mode for Media Plane Security Negotiations	129
Parameters for Media Plane Security Negotiation	129
802.1X Authentication	130
Enable 802.1X Authentication	132
Set Up a Proxy Server	132
Parameters for HTTP Proxy Settings	134
Cisco Product Security Overview	137

---

**CHAPTER 10**

<b>Phone Features and Setup</b>	<b>139</b>
Phone Features and Setup Overview	140
Cisco IP Phone User Support	140
Telephony Features	141
Feature Buttons and Softkeys	149
Assign a Speed Dial Number	150
DTMF Wait and Pause Parameters	150
Enable Conference Button with a Star Code	152
Conference Button Parameters	152
Configure Alphanumeric Dialing	153
Set the Optional Network Configuration	154
Parameters for Optional Network Configuration	154
XML Services	158
XML Directory Service	159



Configure a Phone to Connect to an XML Application	159
Parameters for XML Applications	160
Macro Variables	162
Shared Lines	164
Configure a Shared Line	165
Parameters for Configuring a Shared Line	166
Add Dialog-Based Shared Line Appearance	168
Assign a Ringtone to an Extension	168
Parameters for Ringtone	169
Add Distinctive Ringtone	170
Enable Hoteling on a Phone	171
Enable Flexible Seating on a Phone	172
Enable Extension Mobility on a Phone	172
Set the User Password	173
Download Problem Reporting Tool Logs	174
Configure Problem Report Tool	174
Parameters for Configure Problem Report Tool	176
Server-Configured Paging	178
Configure Multicast Paging	178
Parameters for Multiple Paging Group	179
Configure a Phone to Accept Pages Automatically	182
Manage Phones with TR-069	182
View TR-069 Status	183
Parameters for TR-069 Configuration	184
Set up a Secure Extension	189
Configure the SIP Transport	189
Block Non-Proxy SIP Messages to a Phone	190
Configure a Privacy Header	191
Enable P-Early-Media Support	192
Enable Peer Firmware Sharing	192
Specify the Profile Authentication Type	194
Control the Authentication Requirement to Access the Phone Menus	195
Parameters for User Authentication Control	195
Silence an Incoming Call with Ignore Soft Key	197

Move an Active Call from a Phone to Other Phones (Locations)	197
Parameters for Moving Active Call to Other Locations	199
Sync the Block Caller ID Feature with the Phone and the BroadWorks XSI Server	201
Enable Viewing BroadWorks XSI Call Logs on a Line	202
Parameters for BroadWorks XSI Call Logs on a Line	203
Enable Feature Key Sync	205
DND and Call Forward Status Sync	206
Enable Call Forward Status Sync via XSI Service	207
Enable DND Status Sync via XSI Service	208
Enable Synchronization of Anonymous Call Rejection via XSI Service	208
Set Feature Activation Code for Anonymous Call Rejection	209
Enable Synchronization of Call Waiting via XSI Service	210
Set Feature Activation Code for Call Waiting	211
Enable End-of-Call Statistics Reports in SIP Messages	212
Attributes for Call Statistics in SIP Messages	213
SIP Session ID	214
Enable SIP Session ID	215
Session ID Parameters	216
Set Up a Phone for Remote SDK	216
WebSocket API Parameters	217
Hide a Menu Item from Being Displayed on the Phone Screen	218
Parameters for Menu Visibility	219
Display Caller Number Instead of Unresolved Caller Name	221
Menu Shortcuts Mapping on PSK	222
Add a Menu Shortcut to a Programmable Softkey	225
Enable LDAP Unified Search	226
<b>CHAPTER 11</b>	<b>Phone Information and Display Configuration</b>
	227
Phone Information and Display Settings	227
Configure the Phone Name	227
Customize the Startup Screen	228
Customize Wallpaper for the Phone Display	229
Configure the Screen Saver with the Phone Web Interface	230
Parameters for Screen Saver	231

Adjust Backlight Timer from the Phone Web Interface	233
Customize the Product Configuration Version	234
Keep Focus on the Active Call	234

---

**CHAPTER 12**
**Call Features Configuration 237**

Enable Call Transfer	237
Parameters for Enable Call Transfer	238
Call Forward	239
Enable Call Forward on Voice Tab	239
Parameters for Enable Call Forward on Voice Tab	240
Enable Call Forward on User Tab	241
Parameters for Enable Call Forward on User Tab	242
Enable Feature Activation Code Synchronization for Forward All Calls	245
Set Feature Activation Code for the Call Forward All Service	246
Enable Conferencing	247
Enable Remote Call Recording with SIP REC	247
Enable Remote Call Recording with SIP INFO	249
Configure Missed Call Indication	250
Enable Do Not Disturb	250
Enable Synchronization of Settings Between the Phone and the Server	251
Enable Webex Contacts on the Phone	252
Configure Webex Contacts on a Line Key	253
Add a Softkey for Webex Contacts	254
Enable Webex Call Logs on the Phone	255
Configure Star Codes for DND	255
Set Up a Call Center Agent Phone	256
Parameters for Call Center Agent Setup	257
Restore the ACD Status	259
Display or Hide Unavailable Menu Text Box of Agent Status on the Phone	260
Set Up a Phone for Presence	261
Parameters for Set Up Presence	261
Configure the Number of Call Appearances Per Line	264
Enable Reverse Name Lookup	264
Emergency Calls	266

- Emergency Call Support Background 266
- Emergency Call Support Terminology 267
- Configure a Phone to Make Emergency Calls 267
  - Parameters to Make an Emergency Call 268
- Spam Indication for Incoming Webex Calls 270
- Programmable Softkeys Configuration 271
  - Customize Display of the Softkeys 271
    - Parameters for Programmable Softkeys 271
  - Customize a Programmable Softkey 273
  - Configure Speed Dial on a Programmable Softkey 273
  - Configure a PSK with DTMF Support 274
  - Enable Softkeys to Calls History List Menu 276
  - Spam Indication for Incoming Calls 277
  - Programmable Softkeys 278

---

**CHAPTER 13**

**Audio Configuration 283**

- Configure Different Audio Volume 283
  - Parameters for Audio Volume 283
- Configure the Voice Codecs 284
  - Audio Codec Parameters 285
- Voice Quality Reporting 289
  - Supported Scenarios for Voice Quality Reporting 289
  - Mean Opinion Scores and Codecs 289
  - Configure Voice Quality Reporting 289
    - VQM SIP Publish Message Parameters 290

---

**CHAPTER 14**

**Voicemail Configuration 293**

- Configure Voicemail 293
  - Configure Voicemail for An Extension 293
    - Parameters for Voicemail Server 294

---

**CHAPTER 15**

**Corporate and Personal Directory Setup 297**

- Configure Directory Services 297
  - Parameters for Directory Services 297

Disable Contact Search in All Directories	300
Disable Personal Directory	300
LDAP Configuration	301
Prepare the LDAP Corporate Directory Search	301
Parameters for LDAP Directory	301
Overview of LDAP Directory Access	310
Configure BroadSoft Settings	311
Parameters for XSI Phone Service	312
Set up Personal Directory	322
Enable Reverse Name Lookup	323

---

**PART III**
**Cisco IP Phone Installation 325**


---

**CHAPTER 16**
**Cisco IP Phone Installation 327**

Verify the Network Setup	327
Install the Conference Phone (8832)	328
Ways to Provide Power to Your Conference Phone	329
Configure the Network from the Phone	329
Network Configuration Fields	330
Text and Menu Entry From the Phone	335
Verify Phone Startup	336
Disable or Enable DF Bit	336
Configure Internet Connection Type	337
Configure VLAN Settings	338
VLAN Settings Parameters	339
SIP Configuration	341
Configure the Basic SIP Parameters	341
SIP Parameters	342
Configure the SIP Timer Values	350
SIP Timer Values (sec)	351
Configure the Response Status Code Handling	353
Response Status Code Handling Paramters	354
Configure NTP Server	355
NTP Server Parameters	355

Configure the RTP Parameters	356
RTP Parameters	357
Enable SSRC Reset for the New RTP and SRTP Sessions	360
Control SIP and RTP Behaviour in Dual Mode	361
Configure the SDP Payload Types	363
SDP Payload Types	364
Configure the SIP Settings for Extensions	368
Parameters for SIP Settings on Extensions	369
Configure the SIP Proxy Server	379
SIP Proxy and Registration for Extension Parameters	379
Configure the Subscriber Information Parameters	385
Subscriber Information Parameters	386
Set Up Your Phone to Use OPUS Codec Narrowband	388
NAT Transversal with Phones	388
Enable NAT Mapping	389
NAT Mapping Parameters	390
Configure NAT Mapping with the Static IP Address	391
NAT Mapping with Static IP Parameters	392
Configure NAT mapping with STUN	395
NAT Mapping with STUN Parameters	396
Determine Symmetric or Asymmetric NAT	396
Dial Plan	397
Dial Plan Overview	397
Digit Sequences	398
Digit Sequence Examples	399
Acceptance and Transmission of the Dialed Digits	401
Dial Plan Timer (Off-Hook Timer)	401
Interdigit Long Timer (Incomplete Entry Timer)	402
Interdigit Short Timer (Complete Entry Timer)	403
Edit the Dial Plan on the IP Phone	404
Regional Parameters Configuration	404
Regional Parameters	404
Set the Control Timer Values	405
Parameters for Control Timer Values (sec)	405

Localize Your Cisco IP Phone	407
Configure Time and Date on Phone Web Page	407
Configure Time and Date on the Phone	408
Time and Date Settings	408
Configure Daylight Saving Time	411
Phone Display Language	412
Vertical Service Activation Codes	417
Cisco IP Conference Phone 8832 Multiplatform Phones Documentation	421

---

**PART IV**
**Troubleshooting 423**


---

**CHAPTER 17**
**Troubleshooting 425**

Feature Troubleshooting	425
ACD Call Information Missing	425
Phone Doesn't Show ACD Softkeys	425
Phone Doesn't Show ACD Agent Availability	426
Call Doesn't Record	426
An Emergency Call Doesn't Connect to Emergency Services	427
Presence Status Doesn't Work	427
Phone Presence Message: Disconnected from Server	427
Phone Cannot Access BroadSoft Directory for XSI	428
Phone Doesn't Show Contacts	428
Phone Failed to Upload the PRT Logs to the Remote Server	428
Saved Passwords Become Invalid after Downgrade	429
Failed to Onboard the Phone to Webex	430
Phone Display Problems	430
Phone Displays Irregular Fonts	430
Phone Screen Displays Boxes Instead of Asian Characters	431
Report All Phone Issues from Phone Web Page	431
Report Phone Issues from Webex Control Hub	432
Factory Reset the Phone from Phone Web Page	432
Reboot the Phone from the Webex Control Hub	433
Report a Phone Problem Remotely	433
Capture Packets	434

Voice Quality Troubleshooting Tips 434  
 Phone Behavior During Times of Network Congestion 435  
 Where to Find Additional Information 435

---

**CHAPTER 18**

**Monitoring Phone Systems 437**

Monitoring Phone Systems Overview 437  
 Cisco IP Phone Status 437  
     Display the Phone Information Window 438  
     View Phone Information 438  
     View the Phone Status 439  
     View the Status Messages on the Phone 439  
     View Download Status 439  
     Determine the IP Address of the Phone 440  
     View the Network Status 440  
     Voice Quality Monitoring 441  
     Display Call Statistics Screen 441  
         Call Statistics Fields 441  
     View the Customization State in the Configuration Utility 442  
 Reboot Reasons 443  
     Reboot History on the Phone Web User Interface 443  
     Reboot History on the Cisco IP Phone Screen 444  
     Reboot History in the Status Dump File 444

---

**CHAPTER 19**

**Maintenance 445**

Basic Reset 445  
     Factory Reset the Phone with the Keypad 446  
     Perform Factory Reset from Phone Menu 447  
     Factory Reset the Phone from Phone Web Page 447  
     Identify Phone Issues with a URL in the Phone Web Page 448

---

**APPENDIX A**

**Technical Details 449**

Network Protocols 449  
 Phone Behavior During Times of Network Congestion 453  
 SIP and NAT Configuration 453



SIP and the Cisco IP Phone	453
SIP Over TCP	453
SIP Proxy Redundancy	453
Dual Registration	457
RFC3311	457
SIP NOTIFY XML-Service	457
NAT Transversal with Phones	458
NAT Mapping with Session Border Controller	458
NAT Mapping with SIP-ALG Router	458
Cisco Discovery Protocol	458
LLDP-MED	459
Chassis ID TLV	460
Port ID TLV	460
Time to Live TLV	460
End of LLDPDU TLV	461
Port Description TLV	461
System Name TLV	461
System Capabilities TLV	461
Management Address TLV	461
System Description TLV	461
IEEE 802.3 MAC/PHY Configuration/Status TLV	462
LLDP-MED Capabilities TLV	462
Network Policy TLV	463
LLDP-MED Extended Power-Via-MDI TLV	463
LLDP-MED Inventory Management TLV	463
Final Network Policy Resolution and QoS	464
Special VLANs	464
Default QoS for SIP Mode	464
QoS Resolution for CDP	464
QoS Resolution for LLDP-MED	464
Coexistence with CDP	465
LLDP-MED and Multiple Network Devices	465

---

**APPENDIX B**
**TR-069 Parameter Comparison** 467

[XML and TR-069 Parameter Comparison](#) 467



# CHAPTER 1

## Cisco IP Conference Phone Hardware

- [Cisco IP Conference Phone 8832, on page 1](#)
- [Phones Supported in this Document, on page 3](#)
- [Cisco IP Conference Phone 8832 Buttons and Hardware, on page 3](#)
- [Cisco IP Conference Phone 8832 Documentation, on page 6](#)
- [Terminology Differences, on page 6](#)

### Cisco IP Conference Phone 8832

The Cisco IP Conference Phone 8832 enhances people-centric communications. It combines superior high-definition (HD) audio performance and 360-degree coverage for medium to large conference rooms and executive offices. It provides an audiophile sound experience with a full-duplex two-way wideband (G.722) audio hands-free speaker. This phone is a simple solution that meets the challenges of the most diverse rooms

*Figure 1: Cisco IP Conference Phone 8832 with Multiplatform Firmware*



The conference phone has sensitive microphones with 360-degree coverage. This coverage lets you speak in a normal voice and be heard clearly from up to 10 feet (3 m) away. The phone also features technology that resists interference from mobile phones and other wireless devices, which assures delivery of clear communications without distractions. The phone provides a color screen and softkey buttons to access user

functions. With the base unit alone, the phone provides coverage for a 20 x 20 ft. (6.1 x 6.1 m) room and up to 10 people.

Two wired expansion microphones are available for use with the phone. Placing the expansion microphones away from the base unit provides greater coverage in larger conference rooms. With the base unit and wired expansion microphones, the conference phone provides coverage for a 20 x 34 ft. (6.1 x 10 m) room and up to 22 people.

The phone also supports an optional set of two wireless expansion microphones. With the base unit and wireless expansion microphones, the conference phone provides coverage for a 20 x 40 ft. (6.1 x 12.2 m) room and up to 26 people. To cover a 20 x 40 ft. room, we recommend that you place each microphone at a maximum distance of 10 ft. from the base.

Like other devices, a Cisco IP Phone must be configured and managed. These phones encode and decode the following codecs:

- G.711 a-law
- G.711 mu-law
- G.722
- G722.2 AMR-WB
- G729a
- iLBC
- Opus



---

**Note** Using a cell, mobile, or GSM phone, or two-way radio in close proximity to a Cisco IP Phone might cause interference. For more information, see the manufacturer's documentation of the interfering device.

---

Cisco IP Phones provide traditional telephony functionality, such as call forwarding and transferring, redialing, speed dialing, conference calling, and voice messaging system access. Cisco IP Phones also provide a variety of other features.

As with other network devices, you must configure Cisco IP Phones to prepare them to access the third-party server and the rest of the IP network. By using DHCP, you have fewer settings to configure on a phone. If your network requires it, however, you can manually configure information such as: an IP address, TFTP server, and subnet information.

Cisco IP Phones can interact with other services and devices on your IP network to provide enhanced functionality. For example, you can integrate the third-party server with the corporate Lightweight Directory Access Protocol 3 (LDAP3) standard directory to enable users to search for coworker contact information directly from their IP phones.

Finally, because the Cisco IP Phone is a network device, you can obtain detailed status information from it directly. This information can assist you with troubleshooting any problems users might encounter when using their IP phones. You can also obtain statistics about an active call or firmware versions on the phone.

To function in the IP telephony network, the Cisco IP Phone must connect to a network device, such as a Cisco Catalyst switch. You must also register the Cisco IP Phone with a third-party server before sending and receiving calls.

# Phones Supported in this Document

This document supports these phones:

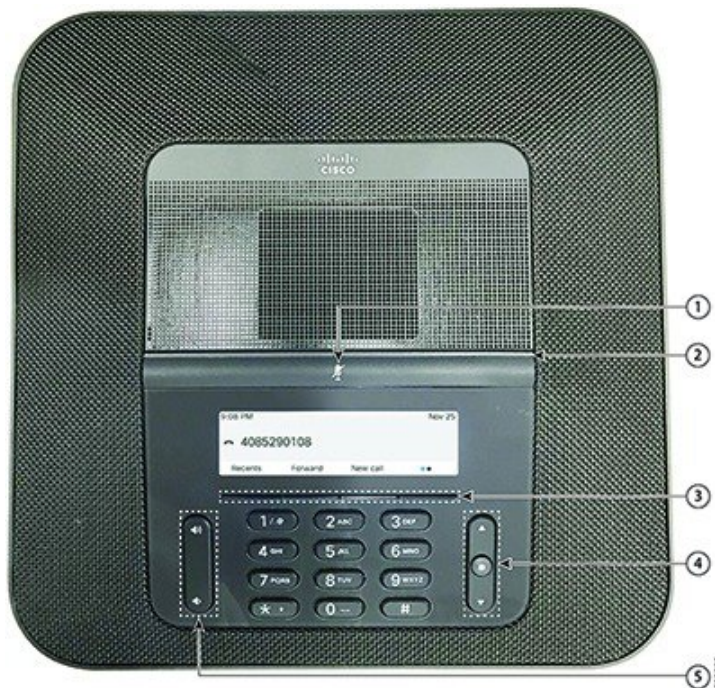
- Cisco IP Conference Phone 8832 Multiplatform Phones



In this document, the term *phone* or *Cisco IP Phone* refers to the above phones.



## Cisco IP Conference Phone 8832 Buttons and Hardware

The following figure shows the Cisco IP Conference Phone 8832.

**Figure 2: Cisco IP Conference Phone 8832 Buttons and Features**



1	Mute bar	 Toggle the microphone on or off. When the microphone is muted, the LED bar is lit red.
2	LED bar	Indicates call states: <ul style="list-style-type: none"> <li>• Green, solid—Active call</li> <li>• Green, flashing—Incoming call</li> <li>• Green, pulsing—Held call</li> <li>• Red, solid—Muted call</li> </ul>
3	Softkey buttons	 Access functions and services.

4	Navigation bar and <b>Select</b> button	 <p>Scroll through menus, highlight items, and select the highlighted item.</p> <p>When the phone is idle, press <b>Up</b> to access the recent calls list and press <b>Down</b> to access the favorites list.</p>
5	<b>Volume</b> button	 <p>Adjust the speakerphone volume (off hook) and the ringer volume (on hook).</p> <p>When you change the volume, the LED bar lights white to show the volume change.</p>

## Conference Phone Softkeys

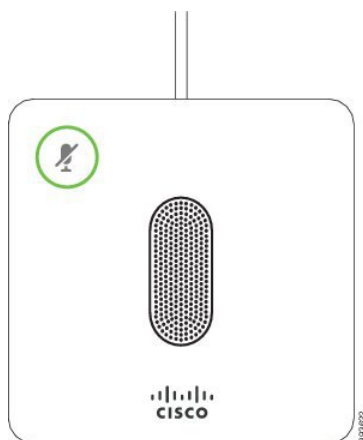
You can interact with the features on your phone with the softkeys. Softkeys, located below the screen, give you access to the function displayed on the screen above the softkey. The softkeys change depending on what you are doing at the time.

The ●● and ●● softkeys indicate more softkey functions are available.

## Wired Expansion Microphone

The Cisco IP Conference Phone 8832 supports two wired expansion microphones, available in an optional kit. Use the expansion microphones in larger rooms or in a crowded room. For best results, we recommend that you place the microphones between 3 feet (0.91 m) and 7 feet (2.1 m) away from the phone.

*Figure 3: Wired Expansion Microphone*



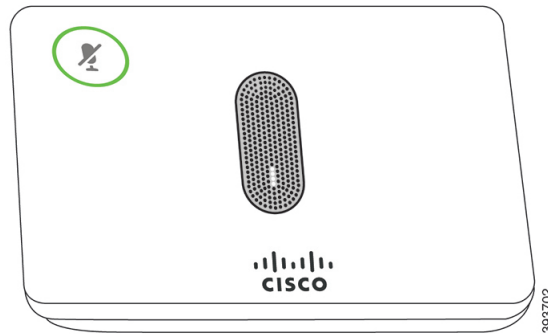
When you're in a call, the expansion microphone LED around the **Mute**  button is green.

When you mute the microphone, the LED is red. When you press the **Mute** button, the phone and the expansion microphones are muted.

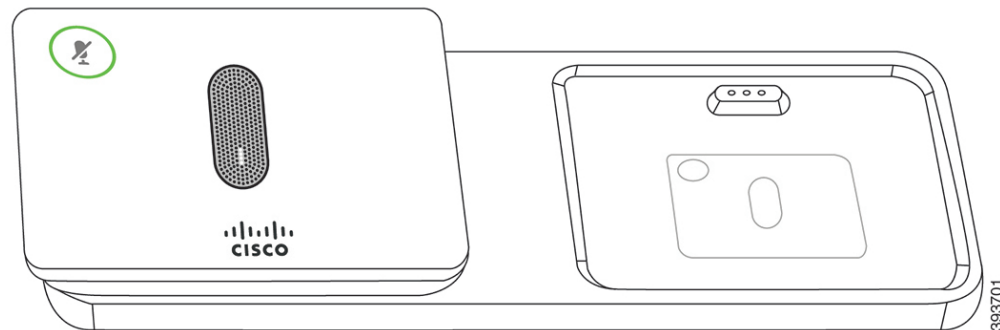
## Wireless Expansion Microphone


The Cisco IP Conference Phone 8832 supports two expansion wireless microphones, available with a charging cradle in an optional kit. When the wireless microphone is placed on the charging cradle for charging, the LED on the cradle is lit white.

**Figure 4: Wireless Microphone**



**Figure 5: Wireless Microphone Mounted on the Charging Cradle**



When the conference phone is in a call, the expansion microphone LED around the **Mute**  button is lit green.

When the microphone is muted, the LED is lit red. When you press the **Mute** button, the phone and the expansion microphones are muted.

If the phone is paired with a wireless microphone (for example, Wireless microphone 1) and you connect the wireless microphone to a charger, pressing the **Show detail** softkey indicates the charge level for that microphone.

When the phone is paired with a wireless microphone and you connect a wired microphone, the wireless microphone gets unpaired and the phone is paired with the wired microphone. A notification appears on the phone screen indicating that the wired microphone is connected.

# Cisco IP Conference Phone 8832 Documentation

Refer to publications that are specific to your language and call control system. Navigate from the following documentation URL:

<https://www.cisco.com/c/en/us/support/collaboration-endpoints/ip-phone-8800-series-multiplatform-firmware/tsd-products-support-series-home.html>

## Terminology Differences

In this document, the term Cisco IP Phone includes the Cisco IP Conference Phone 8832 Multiplatform Phones.

The following table highlights some of the terminology differences in the Cisco IP Conference in the Cisco IP Conference Phone 8832 Multiplatform Phone User Guide, the Cisco IP Conference Phone 8832 Multiplatform Phones Administration Guide.

**Table 1: Terminology Differences**

User Guide	Administration Guide
Message Indicators	Message Waiting Indicator (MWI)
Voicemail System	Voice Messaging System





## CHAPTER 2

# New and Changed Information

- [New and Changed for Firmware Release 11.3\(7\), on page 7](#)
- [New and Changed for Firmware Release 11.3\(6\), on page 8](#)
- [New and Changed for Firmware Release 11.3\(5\), on page 9](#)
- [New and Changed for Firmware Release 11.3\(4\), on page 10](#)
- [New and Changed for Firmware Release 11.3\(3\), on page 10](#)
- [New and Changed for Firmware Release 11.3\(2\), on page 11](#)
- [New and Changed for Firmware Release 11.3\(1\), on page 13](#)
- [New and Changed for Firmware Release 11.2\(3\)SR1, on page 14](#)

## New and Changed for Firmware Release 11.3(7)

Revision	New and Changed
Added the task about how to support Spam indication for incoming calls	<a href="#">Spam Indication for Incoming Webex Calls, on page 270</a>
Updated the topic to add a reference to the topic to “Spam Indication for Incoming Webex Calls”	<a href="#">Spam Indication for Incoming Calls , on page 277</a>
Added the task about how to enable support for LDAP unified search	<a href="#">Enable LDAP Unified Search, on page 226</a>
Updated the topic to mention the general call records that the users can view	<a href="#">Display Call Statistics Screen, on page 441</a>
Updated the topic to update the table	<a href="#">Call Statistics Fields, on page 441</a>
Updated the topic to add more steps	<a href="#">Set the User Password, on page 173</a>
Added the task about how to set up a proxy server in the phone web page	<a href="#">Set Up a Proxy Server, on page 132</a>
Added the topic for the feature <code>HTTP Proxy Support</code>	<a href="#">Parameters for HTTP Proxy Settings, on page 134</a>
Updated the topic to add the feature <code>HTTP Proxy</code>	<a href="#">Telephony Features, on page 141</a>

Revision	New and Changed
Updated the topic to add the shortcut string of the phone menu <b>HTTP proxy settings</b>	<a href="#">Menu Shortcuts Mapping on PSK, on page 222</a>
Updated the topic to add new fields of the feature <code>HTTP Proxy</code>	<a href="#">Network Configuration Fields, on page 330</a>
Updated the topics to mention the HTTP proxy settings	<a href="#">Onboard Your Phone with the Activation Code , on page 19</a> <a href="#">Use DNS SRV for HTTP Provisioning, on page 23</a> <a href="#">Enable Auto Provisioning with Short Activation Code, on page 20</a> <a href="#">Set Up Your Phones for Activation Code Onboarding, on page 48</a>
Added the topic to troubleshoot an issue about the phone onboarding to Webex	<a href="#">Failed to Onboard the Phone to Webex, on page 430</a>

## New and Changed for Firmware Release 11.3(6)

Revision	New and Changed
Updated the task to add the situations in which the focus moves to the incoming call	<a href="#">Keep Focus on the Active Call, on page 234</a>
Updated the description of <code>Call Forward</code>	<a href="#">Telephony Features, on page 141</a>
Updated the topic to add the new parameter <code>Forward Softkey</code>	<a href="#">Parameters for Enable Call Forward on User Tab, on page 242</a>
Updated the softkey in the topic for the new feature	<a href="#">Enable Feature Activation Code Synchronization for Forward All Calls, on page 245</a>
Updated the topic to add the support for French (Canada) language.	<a href="#">Setup for Latin and Cyrillic Languages, on page 414</a>
	<a href="#">Supported Languages for the Phone Display, on page 412</a>
	<a href="#">Set Up Dictionaries and Fonts, on page 413</a>
Updated the description of the parameter <code>Display Attrs</code>	<a href="#">Parameters for LDAP Directory, on page 301</a>
Added the new topic for Webex cloud onboarding	<a href="#">Phone Onboarding to Webex Cloud , on page 20</a>
	<a href="#">Enable a Phone to Onboarding to Webex Cloud, on page 20</a>

Revision	New and Changed
Added the new topic for PRT generation from Cisco Webex Control Hub	<a href="#">Report Phone Issues from Webex Control Hub, on page 432</a>
Added the new topic to reboot from Cisco Webex Control Hub	<a href="#">Reboot the Phone from the Webex Control Hub, on page 433</a>
Added the new topic for Webex contact support	<a href="#">Enable Webex Contacts on the Phone, on page 252</a>
Added the new topic for Webex contact support on a line key	<a href="#">Configure Webex Contacts on a Line Key, on page 253</a>
Added the new topic for Webex contact support on a softkey	<a href="#">Add a Softkey for Webex Contacts, on page 254</a>
Updated the topic for Webex contact on PSK and PLK	<a href="#">Menu Shortcuts Mapping on PSK, on page 222</a>
Added the new topic for Webex call log support	<a href="#">Enable Webex Call Logs on the Phone, on page 255</a>
Added the new topic about how to resolve a downgrade issue	<a href="#">Saved Passwords Become Invalid after Downgrade, on page 429</a>

## New and Changed for Firmware Release 11.3(5)

Revision	New and Changed
Updated the topic to remove a duplicated sentence	<a href="#">Configure Voicemail, on page 293</a>
Rewrote the topic	<a href="#">Configure Voicemail for An Extension, on page 293</a>
Updated the topic to add new parameters	<a href="#">Parameters for Voicemail Server, on page 294</a>
Added the task about how to enable the feature	<a href="#">Keep Focus on the Active Call, on page 234</a>
Updated the topic to add MIC Cert Refresh Status	<a href="#">View Download Status, on page 439</a>
Added the task about how to renew the MIC certificate	<a href="#">Renew the MIC Certificate, on page 60</a>
Added the topic for the feature MIC Certificate Renewal by SUDI Service	<a href="#">Parameters for MIC Certificate Renewal by SUDI Service, on page 61</a>
Added the topic to support STIR/SHAKEN	<a href="#">Spam Indication for Incoming Calls , on page 277</a>
Added the task for dialog-based shared line	<a href="#">Add Dialog-Based Shared Line Appearance, on page 168</a>
Added the task to support single step migration of MPP phones to enterprise phone	<a href="#">Migrate Your Phone to Enterprise Phone Directly, on page 49</a>

## New and Changed for Firmware Release 11.3(4)

Revision	New and Changed
Added a new topic for RTL language support	<a href="#">Setup for RTL Languages, on page 416</a>
Updated the existing topic with RTL language entries	<a href="#">Supported Languages for the Phone Display, on page 412</a>
Updated the existing topic with RTL language entries	<a href="#">Set Up Dictionaries and Fonts, on page 413</a>
Added the task about how to enable SSRC reset to avoid a call transfer error	<a href="#">Enable SSRC Reset for the New RTP and SRTP Sessions, on page 360</a>
Updated the topic to add the new parameter <code>SSRC Reset</code> on <code>RE-INVITE</code>	<a href="#">RTP Parameters, on page 357</a>
Updated the number of the DNS SRV records	<a href="#">SIP Proxy Redundancy, on page 453</a>
Added the task about how to disable or enable the Don't Fragment Bit feature	<a href="#">Disable or Enable DF Bit, on page 336</a>

## New and Changed for Firmware Release 11.3(3)

Revision	New and Changed
Updated the topic to add the new parameter <code>Add Contacts to Directory Personal</code>	<a href="#">Parameters for XSI Phone Service, on page 312</a>
Added the topics for the <code>Synchronization of Call Waiting and Anonymous Call Rejection</code> feature	<a href="#">Enable Synchronization of Anonymous Call Rejection via XSI Service, on page 208</a> <a href="#">Set Feature Activation Code for Anonymous Call Rejection, on page 209</a> <a href="#">Enable Synchronization of Call Waiting via XSI Service, on page 210</a> <a href="#">Set Feature Activation Code for Call Waiting, on page 211</a>
Added the task topic on how to display or hide the <b>Unavailability</b> menu text box of agent status on the phone	<a href="#">Display or Hide Unavailable Menu Text Box of Agent Status on the Phone , on page 260</a>
Added the task topic on how to configure softkeys for different types of calls history list	<a href="#">Enable Softkeys to Calls History List Menu, on page 276</a>
Updated the topic to add new parameters <code>PRT HTTP Header</code> and <code>PRT HTTP Header Value</code>	<a href="#">Parameters for Configure Problem Report Tool, on page 176</a>

Revision	New and Changed
Updated the topic to add the parameter <code>PreconditionSupport</code> and update the parameter <code>SIP_100REL_Enable</code>	<a href="#">Parameters for SIP Settings on Extensions, on page 369</a>
Updated the topic for the <b>Product information</b> screen on the phone	<a href="#">Display the Phone Information Window, on page 438</a>
Added the topic on how to customize the product configuration version	<a href="#">Customize the Product Configuration Version, on page 234</a>

## New and Changed for Firmware Release 11.3(2)

Revision	New and Changed
Added the tasks about the menu shortcuts of features on PSK	<a href="#">Menu Shortcuts Mapping on PSK, on page 222</a> <a href="#">Add a Menu Shortcut to a Programmable Softkey, on page 225</a>
Added the topics for the user authentication control feature	<a href="#">Control the Authentication Requirement to Access the Phone Menus , on page 195</a> <a href="#">Parameters for User Authentication Control, on page 195</a>
Updated the topics about features on PLK and PSK with menu shortcuts	<a href="#">Parameters for Programmable Softkeys, on page 271</a>
Added the topics for the Feature Activation Code Synchronization feature	<a href="#">Enable Feature Activation Code Synchronization for Forward All Calls, on page 245</a> <a href="#">Set Feature Activation Code for the Call Forward All Service, on page 246</a>
Added the topics introducing the SIP Proxy Redundancy enhancements	<a href="#">SIP Proxy Redundancy, on page 453</a> <a href="#">SIP Proxy Failover, on page 454</a> <a href="#">SIP Proxy Fallback, on page 455</a>
Updated the task context to support the SIP proxy redundancy enhancement	<a href="#">Configure the SIP Transport, on page 189</a>
Updated the description for the feature of Show Caller Name and Caller Number	<a href="#">Telephony Features, on page 141</a>
Added the task about configuring the caller name and number display in incoming call alerts	<a href="#">Display Caller Number Instead of Unresolved Caller Name, on page 221</a>
Added the task about how to disable contact search in all directories	<a href="#">Disable Contact Search in All Directories, on page 300</a>

Revision	New and Changed
Added the task about how to disable the personal directory	<a href="#">Disable Personal Directory, on page 300</a>
Added the task about how to hide menu items on the phone screen	<a href="#">Hide a Menu Item from Being Displayed on the Phone Screen, on page 218</a>
Add the reference topic about the menu visibility function	<a href="#">Parameters for Menu Visibility, on page 219</a>
Added the task about how to configure the directory services on the phone web page	<a href="#">Configure Directory Services, on page 297</a>
Added the reference topic about the directory services	<a href="#">Parameters for Directory Services, on page 297</a>
Updated the reference topic to add the new parameters for the directory enhancement feature	<a href="#">Parameters for XSI Phone Service, on page 312</a>
Updated the reference topic for the directory enhancement feature	<a href="#">Feature Buttons and Softkeys, on page 149</a>
Added the reference topic about a troubleshooting case for the directory enhancement feature	<a href="#">Phone Doesn't Show Contacts, on page 428</a>
Updated the task to add more information about how to enable call forward setting on user tab	<a href="#">Enable Call Forward on User Tab, on page 241</a>
Added the reference topic about the parameters for call forward settings on user tab	<a href="#">Parameters for Enable Call Forward on User Tab, on page 242</a>
Updated the reference topic to add new features	<a href="#">Feature Buttons and Softkeys, on page 149</a>
Updated the topic to support the automatic RTP (Real-time Transport Protocol) transport selection	<a href="#">Set up a Secure Extension, on page 189</a>
Updated the Client DN, User Name, Password, and Auth Method parameters for LDAP directory	<a href="#">Parameters for LDAP Directory, on page 301</a>
Added the topic to show the logic of the LDAP directory access	<a href="#">Overview of LDAP Directory Access, on page 310</a>
Updated the firmware version (SWVER) format	<a href="#">Macro Expansion Variables, on page 69</a> <a href="#">Macro Variables, on page 162</a> <a href="#">Conditional Expressions, on page 79</a>
Updated the topic to add prerequisites and updated the short description	<a href="#">Enable Hoteling on a Phone, on page 171</a>
Added the topic to describe the Flexible Seating feature of BroadWorks and how to enable it	<a href="#">Enable Flexible Seating on a Phone, on page 172</a>
Added the topic on how to enable EM for the user	<a href="#">Enable Extension Mobility on a Phone, on page 172</a>

Revision	New and Changed
Updated the topic to support the reverse name lookup against local contacts for BroadWorks server call logs	<a href="#">Enable Viewing BroadWorks XSI Call Logs on a Line</a> , on page 202
Added the task on how to configure StartTLS	<a href="#">Configure StartTLS</a> , on page 118
Updated the topic to add “StartTLS”	<a href="#">Enable Hostname Verification for SIP over TLS</a> , on page 128
Updated the topic to add the new parameter of the feature	<a href="#">Configure the Cipher List</a> , on page 125
Updated the topic for “StartTLS”	<a href="#">Parameters for LDAP Directory</a> , on page 301
Updated the topic for “StartTLS”	<a href="#">XML and TR-069 Parameter Comparison</a> , on page 467
Updated the topic to support the reverse name lookup	<a href="#">Enable Reverse Name Lookup</a> , on page 264
Updated the topic to add the new parameter of the feature	<a href="#">Parameters for Call Center Agent Setup</a> , on page 257
Added the task for the ACD feature sync	<a href="#">Restore the ACD Status</a> , on page 259

## New and Changed for Firmware Release 11.3(1)

Revision	New and Changed
Added a new task to support the feature Auto Provisioning with Short Activation Code.	<a href="#">Enable Auto Provisioning with Short Activation Code</a>
Added topics to support HTTP provisioning with DNS servers	<a href="#">DNS SRV for HTTP Provisioning</a>
Add tasks to support MPP OS Hardening	<a href="#">Enable the Firewall</a> <a href="#">Configure Your Firewall with Additional Options</a>
Added a new task about how to configure a cipher list	<a href="#">Configure the Cipher List</a>
Added a task and the relevant parameters to support client-initiated mode for media plane security negotiations	<a href="#">Enable Client-Initiated Mode for Media Plane Security Negotiations</a>
Added a task about how to enable hostname verification for a line that uses SIP over TLS	<a href="#">Enable Hostname Verification for SIP over TLS</a>
Added a task to support One-Button Call Park.	<a href="#">Configure One-Button Call Park</a>

Revision	New and Changed
Added a task and the parameter about multicast paging	Configure Multicast Paging Parameters for Multiple Paging Group
Added a task and the relevant parameters to support the remote SDK feature	Set Up a Phone for Remote SDK WebSocket API Parameters
Add Task for configuring a programmable softkey (PSK) with DTMF support.	Configure a PSK with DTMF Support
Added a task about how to enable call statistics report in SIP BYE messages	Enable End-of-Call Statistics Reports in SIP Messages
Added a task to support the new feature VQM SIP Publish Message New Fields	Configure Voice Quality Reporting
Added new topics to support the SIP Session ID feature	SIP Session ID Enable SIP Session ID Session ID Parameters
Added description for the new field <i>RTP Before ACK</i>	RTP Parameters
Updated the task on how to configure the SDP Payload Types	Configure the SDP Payload Types
Added a task to support OPUS Codec Narrowband.	Set Up Your Phone to Use OPUS Codec Narrowband

## New and Changed for Firmware Release 11.2(3)SR1

Revision	New and Changed
Added a new task to support Activation Code Onboarding	Activation Code Onboarding





## PART I

# Cisco IP Phone Provisioning

- [Provisioning, on page 17](#)
- [Provisioning Methods, on page 33](#)
- [Provisioning Parameters, on page 63](#)
- [Provisioning Formats, on page 73](#)





## CHAPTER 3

# Provisioning

---

- [Provisioning Overview, on page 17](#)
- [Provisioning, on page 18](#)
- [TR69 Provisioning, on page 25](#)
- [Communication Encryption, on page 26](#)
- [Phone Behavior During Times of Network Congestion, on page 26](#)
- [In-House Preprovisioning and Provisioning Servers, on page 26](#)
- [Server Preparation and Software Tools, on page 27](#)
- [In-House Device Preprovisioning, on page 29](#)
- [Provisioning Server Setup, on page 29](#)

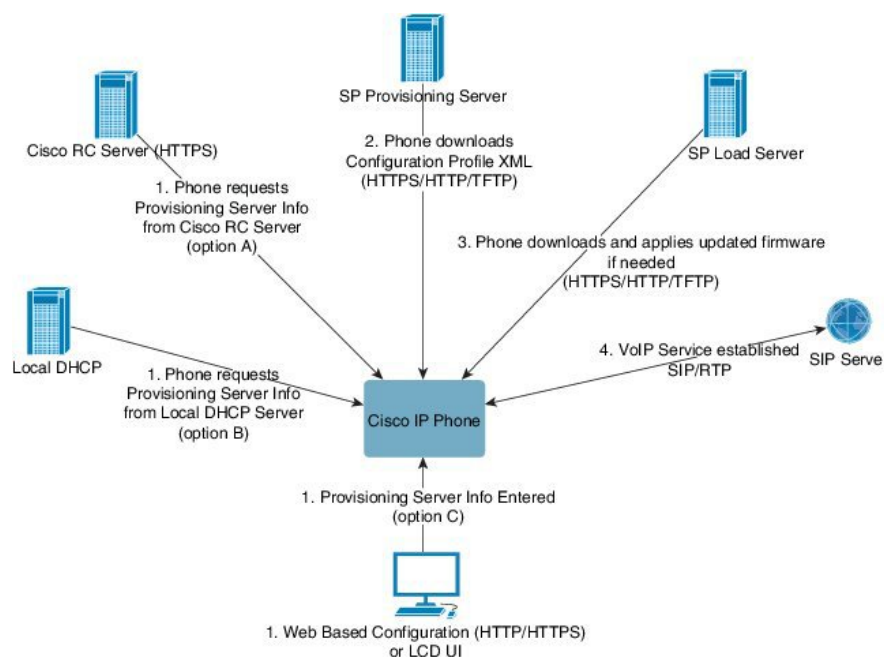
## Provisioning Overview

Cisco IP Phones are intended for high-volume deployments by Voice-over-IP (VoIP) service providers to customers in home, business, or enterprise environments. Hence, provisioning the phone using remote management and configuration ensures the proper operation of the phone at the customer site.

Cisco supports the customized, ongoing feature configuration of the phone by using:

- Reliable remote control of the phone.
- Encryption of the communication that controls the phone.
- Streamlined phone account binding.

Phones can be provisioned to download configuration profiles or updated firmware from a remote server. Downloads can happen when the phones are connected to a network, when they are powered up, and at set intervals. Provisioning is typically part of the high-volume, VoIP deployments common by service providers. Configuration profiles or updated firmware is transferred to the device using TFTP, HTTP, or HTTPS.



At a high level, the phone provisioning process is as follows:

1. If the phone is not configured, the provisioning server information is applied to the phone using one of the following options:
  - **A**—Downloaded from the Cisco Enablement Data Orchestration System (EDOS) Remote Customization (RC) server using HTTPS, DNS SRV, GDS (Activation code onboarding), EDOS device activation.
  - **B**—Queried from a local DHCP server.
  - **C**—Entered manually using the Cisco phone web-based configuration utility or Phone UI.
2. The phone downloads the provisioning server information and applies the configuration XML using the HTTPS, HTTP, or TFTP protocol.
3. The phone downloads and applies the updated firmware, if needed, using HTTPS, HTTP, or TFTP.
4. The VoIP service is established using the specified configuration and firmware.

VoIP service providers intend to deploy many phones to residential and small business customers. In business or enterprise environments, phones can serve as terminal nodes. Providers widely distribute these devices across the Internet, which are connected through routers and firewalls at the customer premises.

The phone can be used as a remote extension of the service provider back-end equipment. Remote management and configuration ensure the proper operation of the phone at the customer premises.

## Provisioning

A phone can be configured to resynchronize its internal configuration state to match a remote profile periodically and on power-up. The phone contacts a normal provisioning server (NPS) or an access control server (ACS).

By default, a profile resync is only attempted when the phone is idle. This practice prevents an upgrade that would trigger a software reboot and interrupt a call. If intermediate upgrades are required to reach a current upgrade state from an older release, the upgrade logic can automate multistage upgrades.

## Normal Provisioning Server

The Normal Provisioning Server (NPS) can be a TFTP, HTTP, or HTTPS server. A remote firmware upgrade is achieved by using TFTP or HTTP, or HTTPS, because the firmware does not contain sensitive information.

Although HTTPS is recommended, communication with the NPS does not require the use of a secure protocol because the updated profile can be encrypted by a shared secret key. For more information about utilizing HTTPS, see [Communication Encryption, on page 26](#). Secure first-time provisioning is provided through a mechanism that uses SSL functionality. An unprovisioned phone can receive a 256-bit symmetric key encrypted profile that is targeted for that device.

## Phone Provisioning Practices

Typically, the Cisco IP Phone is configured for provisioning when it first connects to the network. The phone is also provisioned at the scheduled intervals that are set when the service provider or the VAR preprovisions (configures) the phone. Service providers can authorize VARs or advanced users to manually provision the phone by using the phone keypad. You can also configure provisioning using the Phone Web UI.

Check the **Status > Phone Status > Provisioning** from the Phone LCD UI, or Provisioning Status in the **Status** tab of the web-based Configuration Utility.

## Onboard Your Phone with the Activation Code

This feature is available in firmware release 11-2-3MSR1, BroadWorks Application Server Release 22.0 (patch AP.as.22.0.1123.ap368163 and its dependencies). However, you can change phones with older firmware to use this feature. You instruct the phone to upgrade to the new firmware and to use the `gds://` profile rule to trigger the activation code screen. A user enters a 16-digit code in the provided field to onboard the phone automatically.

### Before you begin

Ensure that you allow the `activation.webex.com` service through your firewall to support onboarding via activation code.

If you want to set up a proxy server for the onboarding, ensure that the proxy server is configured correctly. See [Set Up a Proxy Server, on page 132](#).

### Procedure

- Step 1** Edit the phone `config.xml` file in a text or XML editor.
- Step 2** Follow the example below in your `config.xml` file to set the profile rule for Activation Code Onboarding.

```
<?xml version="1.0" encoding="UTF-8"?>
<device>
<flat-profile>
<!-- System Configuration -->
<Profile_Rule ua="na">gds://</Profile_Rule>
<!-- Firmware Upgrade -->
```

```
<Upgrade_Enable ua="na">Yes</Upgrade_Enable>
<Upgrade_Error_Retry_Delay ua="na">3600</Upgrade_Error_Retry_Delay>
<Upgrade_Rule ua="na">http://<server ip address>/sip88xx.11-2-3MSR1-1.loads</Upgrade_Rule>
<!-- <BACKUP_ACS_Password ua="na"/> -->
</flat-profile>
</device>
```

**Note** For the firmware release after the 11.2(3) SR1, the setting of `Firmware Upgrade` is optional.

**Step 3** Save the changes to the config.xml file.

---


## Phone Onboarding to Webex Cloud

Phone onboarding provides a simple and secure way to onboard Webex-aware phones to Webex cloud. You can achieve the onboarding process either with activation code onboarding (GDS) or with phone MAC address (EDOS device activation).

For more information on how to generate the activation code, see *Cisco BroadWorks Partner Configuration Guide, Cisco Multi-Platform Phones*.

For more information on Webex-aware phone onboarding, see *Webex for Cisco BroadWorks Solution Guide*.

## Enable a Phone to Onboarding to Webex Cloud

After the successful registration of the phone to the Webex cloud, a cloud symbol  appears on the phone screen.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

---

**Step 1** Select **Voice > Phone**.

**Step 2** In the **Webex** section, set the **Onboard Enable** parameter to **Yes**.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<Webex_Onboard_Enable ua="na">Yes</Webex_Onboard_Enable>
```

Default value: Yes

**Step 3** Click **Submit All Changes**.

---

## Enable Auto Provisioning with Short Activation Code

Use the steps below to enable auto provisioning with a short activation code.

### Before you begin

Ensure that your phones are updated with Firmware Release 11.3(1) or later.

If you want to set up a proxy server for the phone, ensure that the proxy server is configured correctly. See [Set Up a Proxy Server, on page 132](#).

Review how to set up the CDA server for redirection profile:

<https://community.cisco.com/t5/collaboration-voice-and-video/cisco-multi-platform-phones-cloud-provisioning-process/ta-p/3910244>

### Procedure

---

- Step 1** Create a redirection profile name that contains a any number of digits between three and 16, inclusive. This becomes the activation code, later. Use one of these formats:
- **nnn.**
  - **nnnnnnnnnnnnnnnnnnnn**
  - Any number of digits between three and sixteen, inclusive. Example, **123456**
- Step 2** Provide the profile name that you created in step 1 to the Customer Device Activation (CDA) support team at [cdap-support@cisco.com](mailto:cdap-support@cisco.com).
- Step 3** Ask the CDA support team to enable your profile for discovery.
- Step 4** When you get confirmation from the CDA support team, distribute the activation code to the users.
- Step 5** Instruct users to press pound (#) before entering the digits at the activation screen.
- 

## Manually Provision a Phone from the Keypad

### Procedure

---

- Step 1** Press **Settings**.
- Step 2** Select **Device administration > Profile Rule**.
- Step 3** Enter the profile rule using the following format:

```
protocol://server[:port]/profile_pathname
```

For example:

```
tftp://192.168.1.5/CP_x8xx_MPP.cfg
```

If no protocol is specified, TFTP is assumed. If no server-name is specified, the host that requests the URL is used as the server name. If no port is specified, the default port is used (69 for TFTP, 80 for HTTP, or 443 for HTTPS).

- Step 4** Press **Resync**.
-

## DNS SRV for HTTP Provisioning

The DNS SRV for HTTP Provisioning feature enables auto provisioning of your multiplatform phone. Domain Name System Service (DNS SRV) records establish connections between a service and a hostname. When the phone looks for the location of the provisioning service, it first queries on the given DNS SRV domain name, then it queries for SRV records. The phone validates the records to confirm that the server is accessible. Then, it continues to the actual provisioning flow. Service providers can utilize this DNS SRV provisioning flow to provide auto provisioning.

DNS SRV bases the hostname validation on the certificate of the DHCP provided domain name. It is important that all SRV records use a valid certificate containing the DHCP provided domain name.

The DNS SRV query includes the DHCP domain name in its construction as follows:

**`<_<servicename>.<transport>.<domainName>`**

For example, `_ciscoprov-https._tls.example.com`, instructs the phone to do a lookup for example.com. The phone uses the hostname and port number that's retrieved by the DNS SRV query to build the URL that it uses to download the initial configuration.

DNS SRV is one of many auto provisioning mechanisms that the phone uses. The phone tries the mechanisms in the following order:

1. DHCP
2. DNS SRV
3. EDOS
4. GDS (Activation Code Onboarding), or EDOS Device Activation

The following table describes the SRV record fields.

**Table 2: SRV Record Fields**

Field	Description	Example
<code>&lt;_servicename&gt;</code>	The service name begins with an underscore. Server services use symbolic names in SRV records.  After the service, a period (.) signifies that the service is established and the next section is beginning.	<code>_ciscoprov-https</code> . Or <code>_ciscoprov-http</code> .  DNS SRV doesn't support the TFTP protocol. If you use TFTP, you receive the following error message: Error - TFTP Scheme not supported in SRV lookups.
<code>&lt;_proto&gt;</code>	The transport protocol begins with an underscore.  The period that follows the protocol signals that the protocol section has ended.	<code>_tls</code> . You must use HTTPS with TLS.  Or <code>_tcp</code> . You must use HTTP with TCP.



Field	Description	Example
<domainName>	The service domain name follows the protocol. Hostname validation: All SRV records are validated based on the original DHCP-provided domain name. It is important that all records use a valid certificate containing the original domain name.	<b>example.com</b>
TTL (Time to Live)	Expiration value of the record, in seconds.	86400
Class	Internet-type—Standard BIND notation indicating that it's an SRV record.	IN
<priority>	Each line contains a priority number. The lower the number, the earlier the phone will attempt the target hostname and port included in this DNS SRV record.	<b>10</b>
<weight>	If two or more services have the same priority, the weight number determines which line comes first. The lower the number, the earlier the phone will attempt the target hostname and port included in this DNS SRV record.	<b>20</b>
<port>	optional port number	<b>5060</b>
<target>	The A record of the machine providing the service. A Records are the most basic type of DNS record and are used to point a domain or subdomain to an IP address.	<b>pr1.example.com</b>

### Example SRV Configurations

```

_service._proto.name. TTL class SRV priority weight port target.
_ciscoprov-https._tls.example.com. 86400 IN SRV 10 60 5060 pr1.example.com.
_ciscoprov-https._tls.example.com. 86400 IN SRV 10 20 5060 pr2.example.com.
_ciscoprov-http._tcp.example.com. 86400 IN SRV 10 50 5060 px1.example.com.
_ciscoprov-http._tcp.example.com. 86400 IN SRV 10 30 5060 px2.example.com.

```

## Use DNS SRV for HTTP Provisioning

New phones use DNS SRV as one method of auto provisioning. For existing phones, if your network is set up for provisioning with DNS SRV for HTTP, you can use this feature to resync your phone. Sample configuration file:

```

<flat-profile>
<!-- System Configuration -->
<Primary_DNS ua="rw">10.89.68.150</Primary_DNS>
<Back_Light_Timer ua="rw">Always On</Back_Light_Timer>
<Peer_Firmware_Sharing ua="na">Yes</Peer_Firmware_Sharing>
<Profile_Authentication_Type ua="na">Basic Http Authentication </Profile_Authentication_Type>
<Proxy_1_ ua="na">example.com</Proxy_1_>

```

```
<Display_Name_1_ ua="na">4081001141</Display_Name_1_>
<User_ID_1_ ua="na">4081001141</User_ID_1_>
</flat-profile>
```

### Before you begin

If you want to set up a proxy server for the HTTP provisioning, ensure that the proxy server is configured correctly. See [Set Up a Proxy Server, on page 132](#).

### Procedure

---

Perform one of the following actions. Then, [Set the Profile Rule with the SRV Option on the Web Page, on page 24](#) or [Set the Profile Rule with the SRV Option on the Phone, on page 24](#)

- Place the XML configuration file, \$PSN.xml, in the web server `root` directory.
  - Place the XML configuration file, \$MA.cfg, in the web server `root` directory/`Cisco/`.
- 

## Set the Profile Rule with the SRV Option on the Web Page

You can use the SRV option to download a configuration file to your phone.

### Before you begin

[Access the Phone Web Interface, on page 100](#)

### Procedure

- 
- Step 1** Select **Voice > Provisioning**
- Step 2** In the **Profile Rule** field, enter the profile rule with the SRV option. Only HTTP and HTTPS are supported. Example:
- ```
[--srv] https://example.com/$PSN.xml
```
- 

## Set the Profile Rule with the SRV Option on the Phone

You can use the SRV option on your phone to download a configuration file.

### Procedure

- 
- Step 1** Press **Settings**.
- Step 2** Select **Device administration > Profile rule**.
- Step 3** Enter the profile rule with the `[--srv]` parameter. Only HTTP and HTTPS are supported. Example:
- ```
[--srv] https://example.com/$PSN.xml
```

**Step 4** Press **Resync**.

---

## TR69 Provisioning

The Cisco IP Phone helps the administrator to configure the TR69 parameters using the Web UI. For information related to the parameters, including a comparison of the XML and TR69 parameters, see the Administration Guide for the corresponding phone series.

The phones support Auto Configuration Server (ACS) discovery from DHCP Option 43, 60, and 125.

- Option 43—Vendor-specific information for the ACS URL.
- Option 60—Vendor class identifier, for the phone to identify itself with `dslforum.org` to the ACS.
- Option 125—Vendor-specific information for the gateway association.

## TR69 RPC Methods

### RPC Methods Supported

The phones support only a limited set of Remote Procedure Call (RPC) methods as follows:

- GetRPCMethods
- SetParameterValues
- GetParameterValues
- SetParameterAttributes
- GetParameterAttributes
- GetParameterNames
- AddObject
- DeleteObject
- Reboot
- FactoryReset
- Inform
- Download: Download RPC method, the file types supported are:
  - Firmware upgrade image
  - Vendor configuration file
  - Custom Certificate Authority (CA) file
- Transfer Complete

## Event Types Supported

The phones support event types based on features and methods supported. Only the following event types are supported:

- Bootstrap
- Boot
- value change
- connection request
- Periodic
- Transfer Complete
- M Download
- M Reboot

## Communication Encryption

The configuration parameters that are communicated to the device can contain authorization codes or other information that protect the system from unauthorized access. It is in the service provider's interest to prevent unauthorized customer activity. It is in the customer's interest to prevent the unauthorized use of the account. The service provider can encrypt the configuration profile communication between the provisioning server and the device, in addition to restricting access to the administration web server.

## Phone Behavior During Times of Network Congestion

Anything that degrades network performance can affect phone audio and, in some cases, can cause a call to drop. Sources of network degradation can include, but are not limited to, the following activities:

- Administrative tasks, such as an internal port scan or security scan.
- Attacks that occur on your network, such as a Denial of Service attack.

## In-House Preprovisioning and Provisioning Servers

The service provider preprovisions phones, other than RC units, with a profile. The preprovision profile can comprise a limited set of parameters that resynchronizes the phone. The profile can also comprise a complete set of parameters that the remote server delivers. By default, the phone resynchronizes on power-up and at intervals that are configured in the profile. When the user connects the phone at the customer premises, the device downloads the updated profile and any firmware updates.

This process of preprovisioning, deployment, and remote provisioning can be accomplished in many ways.

# Server Preparation and Software Tools

The examples in this chapter require the availability of one or more servers. These servers can be installed and run on a local PC:

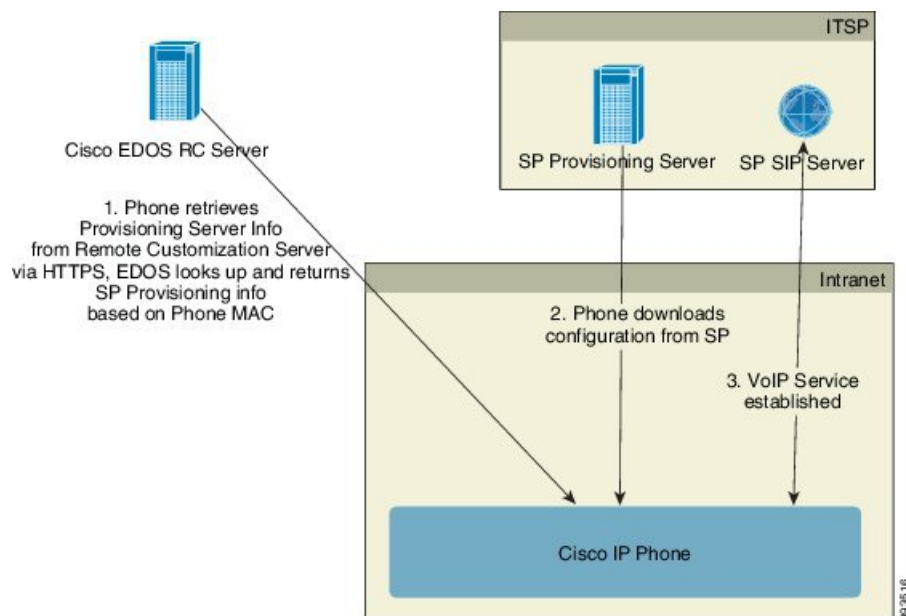
- TFTP (UDP port 69)
- syslog (UDP port 514)
- HTTP (TCP port 80)
- HTTPS (TCP port 443).

To troubleshoot server configuration, it is helpful to install clients for each type of server on a separate server machine. This practice establishes proper server operation, independent of the interaction with the phones.

We also recommend that you install these software tools:

- To generate configuration profiles, install the open source gzip compression utility.
- For profile encryption and HTTPS operations, install the open source OpenSSL software package.
- To test the dynamic profile generation and one-step remote provisioning using HTTPS, we recommend a scripting language with CGI scripting support. Open source Perl language tools is an example of such a scripting language.
- To verify secure exchanges between provisioning servers and the phones, install an Ethernet packet sniffer (such as the freely downloadable Ethereal/Wireshark). Capture an Ethernet packet trace of the interaction between the phone and the provisioning server. To do so, run the packet sniffer on a PC that is connected to a switch with port mirroring enabled. For HTTPS transactions, you can use the ssldump utility.

## Remote Customization (RC) Distribution



All phones contact the Cisco EDOS RC server until they are provisioned initially.

In an RC distribution model, a customer purchases a phone that has already been associated with a specific Service Provider in the Cisco EDOS RC Server. The Internet Telephony Service Provider (ITSP) sets up and maintains a provisioning server, and registers their provisioning server information with the Cisco EDOS RC Server.

When the phone is powered on with an internet connection, the customization state for the unprovisioned phone is **Open**. The phone first queries the local DHCP server for provisioning server information and sets the customization state of the phone. If DHCP query is successful, Customization State is set to **Aborted** and RC is not attempted due to DHCP providing the needed provisioning server information.

When a phone connects to a network for the first time or after a factory reset, if there are no DHCP options setup, it contacts a device activation server for zero touch provisioning. New phones will use “activate.cisco.com” instead of “webapps.cisco.com” for provisioning. Phones with firmware release prior to 11.2(1), will continue to use webapps.cisco.com. Cisco recommends that you allow both the domain names through your firewall.

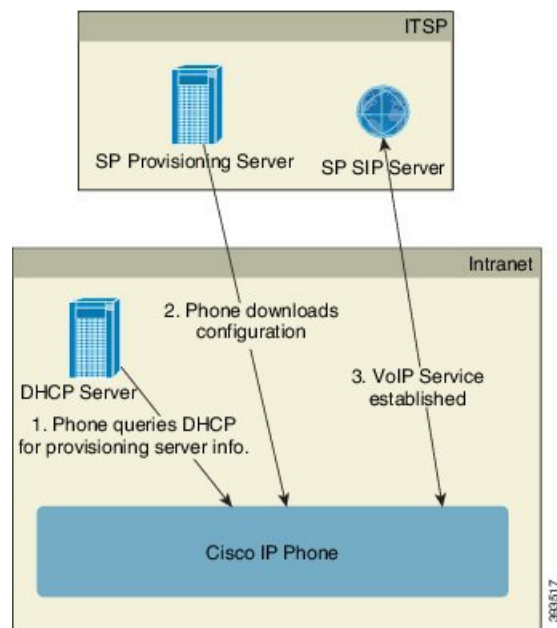
If DHCP server does not provide provisioning server information, the phone queries the Cisco EDOS RC Server and provides its MAC address and model and the Customization State is set to **Pending**. The Cisco EDOS server responds with the associated service provider's provisioning server information including provisioning server URL and the phone's Customization State is set to **Custom Pending**. The phone then performs a resync URL command to retrieve the Service Provider's configuration and, if successful, the Customization State is set to **Acquired**.

If the Cisco EDOS RC Server does not have a service provider associated with the phone, the customization state of the phone is set to **Unavailable**. The phone can be manually configured or an association added for the service provider of the phone to the Cisco EDOS Server.

If a phone is provisioned via either the LCD or Web Configuration Utility, prior to the Customization State becoming **Acquired**, the Customization State is set to **Aborted** and the Cisco EDOS Server will not be queried unless the phone is factory reset.

Once the phone has been provisioned, the Cisco EDOS RC Server is not utilized unless the phone is factory reset.

## In-House Device Preprovisioning



With the Cisco factory default configuration, the phone automatically tries to resync to a profile on a TFTP server. A managed DHCP server on a LAN delivers the information about the profile and TFTP server that is configured for preprovisioning to the device. The service provider connects each new phone to the LAN. The phone automatically resyncs to the local TFTP server and initializes its internal state in preparation for deployment. This preprovisioning profile typically includes the URL of a remote provisioning server. The provisioning server keeps the device updated after the device is deployed and connected to the customer network.

The preprovisioned device bar code can be scanned to record its MAC address or serial number before the phone is shipped to the customer. This information can be used to create the profile to which the phone resynchronizes.

Upon receiving the phone, the customer connects it to the broadband link. On power-up, the phone contacts the provisioning server through the URL that is configured through preprovisioning. The phone can thus resync and update the profile and firmware, as necessary.

## Provisioning Server Setup

This section describes setup requirements for provisioning a phone by using various servers and different scenarios. For the purposes of this document and for testing, provisioning servers are installed and run on a local PC. Also, generally available software tools are useful for provisioning the phones.

## TFTP Provisioning

The phones support TFTP for both provisioning resync and firmware upgrade operations. When devices are deployed remotely, HTTPS is recommended, but HTTP and TFTP can also be used. This then requires provisioning file encryption to add security, as it offers greater reliability, given NAT and router protection mechanisms. TFTP is useful for the in-house preprovisioning of a large number of unprovisioned devices.

The phone is able to obtain a TFTP server IP address directly from the DHCP server through DHCP option 66. If a Profile\_Rule is configured with the filepath of that TFTP server, the device downloads its profile from the TFTP server. The download occurs when the device is connected to a LAN and powered up.

For a device with the factory default profile, upon powering up, the device resyncs to this file on the local TFTP server that DHCP option 66 specifies. The filepath is relative to the TFTP server virtual root directory.

## Remote Endpoint Control and NAT

The phone is compatible with network address translation (NAT) to access the Internet through a router. For enhanced security, the router might attempt to block unauthorized incoming packets by implementing symmetric NAT, a packet-filtering strategy that severely restricts the packets that are allowed to enter the protected network from the Internet. For this reason, remote provisioning by using TFTP is not recommended.

VoIP can coexist with NAT only when some form of NAT traversal is provided. Configure Simple Traversal of UDP through NAT (STUN). This option requires that the user have:

- A dynamic external (public) IP address from your service
- A computer that is running STUN server software
- An edge device with an asymmetric NAT mechanism

## HTTP Provisioning

The phone behaves like a browser that requests web pages from a remote Internet site. This provides a reliable means of reaching the provisioning server, even when a customer router implements symmetric NAT or other protection mechanisms. HTTP and HTTPS work more reliably than TFTP in remote deployments, especially when the deployed units are connected behind residential firewalls or NAT-enabled routers. HTTP and HTTPS are used interchangeably in the following request type descriptions.

Basic HTTP-based provisioning relies on the HTTP GET method to retrieve configuration profiles. Typically, a configuration file is created for each deployed phone, and these files are stored within an HTTP server directory. When the server receives the GET request, it simply returns the file that is specified in the GET request header.

Rather than a static profile, the configuration profile can be generated dynamically by querying a customer database and producing the profile on-the-fly.

When the phone requests a resynch, it can use the HTTP POST method to request the resynch configuration data. The device can be configured to convey certain status and identification information to the server within the body of the HTTP POST request. The server uses this information to generate a desired response configuration profile, or to store the status information for later analysis and tracking.

As part of both GET and POST requests, the phone automatically includes basic identifying information in the User-Agent field of the request header. This information conveys the manufacturer, product name, current firmware version, and product serial number of the device.



User Agent is configurable, and the phone uses this the value if it has not be configured (still at default).

When the phone is configured to resync to a configuration profile by using HTTP, it is recommended that HTTPS be used or the profile be encrypted to protect confidential information. Encrypted profiles that the phone downloads by using HTTP avoid the danger of exposing confidential information that is contained in the configuration profile. This resync mode produces a lower computational load on the provisioning server when compared to using HTTPS.

The phone can decrypt profiles encrypted with one of these encryption methods:

- AES-256-CBC encryption
- RFC-8188 based encryption with AES-128-GCM ciphering



**Note** The phones support HTTP Version 1.0, HTTP Version 1.1, and Chunk Encoding when HTTP Version 1.1 is the negotiated transport protocol.

## HTTP Status Code Handling on Resync and Upgrade

The phone supports HTTP response for remote provisioning (Resync). Current phone behavior is categorized in three ways:

- A—Success, where the “Resync Periodic” and “Resync Random Delay” values determine subsequent requests.
- B—Failure when File Not Found or corrupt profile. The “Resync Error Retry Delay” value determines subsequent requests.
- C—Other failure when a bad URL or IP address causes a connection error. The “Resync Error Retry Delay” value determines subsequent requests.

**Table 3: Phone Behavior for HTTP Responses**

HTTP Status Code	Description	Phone Behavior
<b>301 Moved Permanently</b>	This and future requests should be directed to a new location.	Retry request immediately with new location.
<b>302 Found</b>	Known as Temporarily Moved.	Retry request immediately with new location.
<b>3xx</b>	Other 3xx responses not processed.	C
<b>400 Bad Request</b>	The request cannot be fulfilled due to bad syntax.	C
<b>401 Unauthorized</b>	Basic or digest access authentication challenge.	Immediately retry request with authentication credentials. Maximum 2 retries. Upon failure, the phone behavior is C.
<b>403 Forbidden</b>	Server refuses to respond.	C

HTTP Status Code	Description	Phone Behavior
<b>404 Not Found</b>	Requested resource not found. Subsequent requests by client are permissible.	B
<b>407 Proxy Authentication Required</b>	Basic or digest access authentication challenge.	Immediately retry request with authentication credentials. Maximum two retries. Upon failure, the phone behavior is C.
<b>4xx</b>	Other client error status codes are not processed.	C
<b>500 Internal Server Error</b>	Generic error message.	Phone behavior is C.
<b>501 Not Implemented</b>	The server does not recognize the request method, or it lacks the ability to fulfill the request.	Phone behavior is C.
<b>502 Bad Gateway</b>	The server is acting as a gateway or proxy and receives an invalid response from the upstream server.	Phone behavior is C.
<b>503 Service Unavailable</b>	The server is currently unavailable (overloaded or down for maintenance). This is a temporary state.	Phone behavior is C.
<b>504 Gateway Timeout</b>	The server behaves as a gateway or proxy and does not receive timely response from the upstream server.	C
<b>5xx</b>	Other server error	C



## CHAPTER 4

# Provisioning Methods

---

- Provision a Phone with BroadSoft Server , on page 33
- Provisioning Examples Overview, on page 34
- Basic Resync, on page 34
- TFTP Resync, on page 34
- Unique Profiles, Macro Expansion, and HTTP, on page 38
- Resync a Device Automatically, on page 40
- Set Up Your Phones for Activation Code Onboarding, on page 48
- Migrate Your Phone to Enterprise Phone Directly, on page 49
- Secure HTTPS Resync, on page 50
- Profile Management, on page 57
- Set the Phone Privacy Header, on page 59
- Renew the MIC Certificate, on page 60

## Provision a Phone with BroadSoft Server

BroadSoft Server user only.

You can register your Cisco IP multiplatform phones to a BroadWorks platform.

### Procedure

---

- Step 1** Download the CPE Kit from BroadSoft Xchange. To get the latest CPE kits, go to this URL: <https://xchange.broadsoft.com>.
- Step 2** Upload the most recent DTAF file to the BroadWorks (system level) server.  
For more information, go to this URL: (<https://xchange.broadsoft.com/node/1031047>). Access the *BroadSoft Partner Configuration Guide* and see the section “*Configure BroadWorks Device Profile Type*”.
- Step 3** Configure Broadworks Device Profile Type.  
For more information on how to configure the device profile type, go to this URL: <https://xchange.broadsoft.com/node/1031047>. Access the *BroadSoft Partner Configuration Guide* and see the section “*Broadworks Device Profile Type Configuration*”.
-

# Provisioning Examples Overview

This chapter provides example procedures for transferring configuration profiles between the phone and the provisioning server.

For information about creating configuration profiles, refer to [Provisioning Formats, on page 73](#).

## Basic Resync

This section demonstrates the basic resync functionality of the phones.

## Use Syslog to Log Messages

To get the information, you can access the phone Web interface, select **Info > Debug Info > Control Logs** and click **messages**.

### Before you begin

### Procedure

---

- Step 1** Install and activate a syslog server on the local PC.
- Step 2** Click the **System** tab and enter the value of your local syslog server into the Syslog\_Server parameter.
- Step 3** Repeat the resync operation as described in [TFTP Resync, on page 34](#).

The device generates two syslog messages during the resync. The first message indicates that a request is in progress. The second message marks success or failure of the resync.

- Step 4** Verify that your syslog server received messages similar to the following:

The contents of these messages can be configured by using the following parameters:

If any of these parameters are cleared, the corresponding syslog message is not generated.

---

## TFTP Resync

The phone supports multiple network protocols for retrieving configuration profiles. The most basic profile transfer protocol is TFTP (RFC1350). TFTP is widely used for the provisioning of network devices within private LAN networks. Although not recommended for the deployment of remote endpoints across the Internet, TFTP can be convenient for deployment within small organizations, for in-house preprovisioning, and for development and testing. See [In-House Device Preprovisioning, on page 29](#) for more information on in-house preprovisioning. In the following procedure, a profile is modified after downloading a file from a TFTP server.

## Procedure

---

- Step 1** Within a LAN environment, connect a PC and a phone to a hub, switch, or small router.
- Step 2** On the PC, install and activate a TFTP server.
- Step 3** Use a text editor to create a configuration profile that sets the value for GPP\_A to 12345678 as shown in the example.

```
<flat-profile>
  <GPP_A> 12345678
</GPP_A>
</flat-profile>
```

- Step 4** Save the profile with the name `basic.txt` in the root directory of the TFTP server.
- You can verify that the TFTP server is properly configured: request the `basic.txt` file by using a TFTP client other than the phone. Preferably, use a TFTP client that is running on a separate host from the provisioning server.
- Step 5** Select the **Voice > Provisioning** tab, and inspect the values of the general purpose parameters GPP\_A through GPP\_P. These should be empty.
- Step 6** Resync the test phone to the `basic.txt` configuration profile by opening the resync URL in a web browser window.

If the IP address of the TFTP server is 192.168.1.200, the command should be similar to the following example:

```
http://192.168.1.100/admin/resync?tftp://192.168.1.200/basic.txt
```

When the phone receives this command, the device at address 192.168.1.100 requests the file `basic.txt` from the TFTP server at IP address 192.168.1.200. The phone then parses the downloaded file and updates the GPP\_A parameter with the value 12345678.

- Step 7** Verify that the parameter was correctly updated: Refresh the configuration page on the PC web browser and select the **Voice > Provisioning** tab.

The GPP\_A parameter should now contain the value 12345678.

---

## Log Messages to the Syslog Server

If a syslog server is configured on the phone through the use of the parameters, the resync and upgrade operations send messages to the syslog server. A message can be generated at the start of a remote file request (configuration profile or firmware load), and at the conclusion of the operation (indicating either success or failure).

You can also configure the parameters in the phone configuration file with XML(`cfg.xml`) code. To configure each parameter, see the syntax of the string in [System Log Parameters, on page 36](#).

### Before you begin

- A syslog server is installed and configured.

- Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

- Step 1** Click **Voice > System**.
- Step 2** In the **Optional Network Configuration** section, enter the server IP in **Syslog Server** and optionally specify a **Syslog Identifier** as defined in [System Log Parameters, on page 36](#).
- Step 3** Optionally define the content of the syslog messages using **Log Request Msg**, **Log Success Msg**, and **Log Failure Msg** as defined in [System Log Parameters, on page 36](#).

The fields defining syslog message content are located in the **Configuration Profile** section on the **Voice > Provisioning** tab. If you don't specify the message content, the default settings in the fields are used. If any of the fields are cleared, the corresponding message is not generated.

- Step 4** Click **Submit All Changes** to apply the configuration.
- Step 5** Verify the validity of the configuration.

- a) Perform a TFTP resync. See [TFTP Resync, on page 34](#).

The device generates two syslog messages during the resync. The first message indicates that a request is in progress. The second message marks the success or failure of the resync.

- b) Verify that your syslog server received messages similar to the following:

```
CP-78xx-3PCC 00:0e:08:ab:cd:ef -- Requesting resync tftp://192.168.1.200/basic.txt
CP-88xx-3PCC 00:0e:08:ab:cd:ef -- Successful resync tftp://192.168.1.200/basic.txt
```

## System Log Parameters

The following table defines the function and usage of the syslog parameters in the **Optional Network Configuration** section under the **Voice > System** tab in the phone web page. It also defines the syntax of the string that is added in the phone configuration file (cfg.xml) with XML code to configure a parameter.

**Table 4: Syslog Parameters**

Parameter Name	Description and Default Value
Syslog Server	<p>Specify the server for logging the phone system information and critical events. If both Debug Server and Syslog Server are specified, Syslog messages are also logged to the Debug Server.</p> <ul style="list-style-type: none"> <li>• <b>In the phone configuration file (cfg.xml) with XML</b>, enter a string in this format:  <pre>&lt;Syslog_Server ua="na"&gt;10.74.30.84&lt;/Syslog_Server&gt;</pre> </li> <li>• <b>On the phone web page</b>, specify the Syslog server.</li> </ul>

Parameter Name	Description and Default Value
Syslog Identifier	<p>Select the device identifier to include in syslog messages that are uploaded to the syslog server. The device identifier appears after the timestamp in each message. The options for the identifiers are:</p> <ul style="list-style-type: none"> <li>• None: No device identifier.</li> <li>• \$MA: The MAC address of the phone, expressed as continuous lower case letters and digits. Example: c4b9cd811e29</li> <li>• \$MAU: The MAC address of the phone, expressed as continuous upper case letters and digits. Example: C4B9CD811E29</li> <li>• \$MAC: The MAC address of the phone in the standard colon-separated format. Example: c4:b9:cd:81:1e:29</li> <li>• \$SN: The product serial number of the phone.</li> <li>• <b>In the phone configuration file with XML(cfg.xml)</b>, enter a string in this format:  <pre>&lt;Syslog_Identifier ua="na"&gt;\$MAC&lt;/Syslog_Identifier&gt;</pre> </li> <li>• <b>On the phone web page</b>, select an identifier from the list.</li> </ul> <p>Default: None</p>
Log Request Msg	<p>The message that is sent to the syslog server at the start of a resync attempt. If no value is specified, the syslog message is not generated.</p> <p>The default value is \$PN \$MAC -- Requesting resync  \$SCHEME://\$SERVIP:\$PORT\$PATH</p> <ul style="list-style-type: none"> <li>• <b>In the phone configuration file with XML(cfg.xml)</b>, enter a string in this format:  <pre>&lt;Log_Request_Msg ua="na"&gt;\$PN \$MAC -- Requesting resync  \$SCHEME://\$SERVIP:\$PORT\$PATH&lt;/Log_Request_Msg&gt;</pre> </li> </ul>
Log Success Msg	<p>The syslog message that is issued upon successful completion of a resync attempt. If no value is specified, the syslog message is not generated.</p> <p><b>In the phone configuration file with XML(cfg.xml)</b>, enter a string in this format:  <pre>&lt;Log_Success_Msg ua="na"&gt;\$PN \$MAC -- Successful resync  \$SCHEME://\$SERVIP:\$PORT\$PATH&lt;/Log_Success_Msg&gt;</pre> </p>
Log Failure Msg	<p>The syslog message that is issued after a failed resync attempt. If no value is specified, the syslog message is not generated.</p> <p>The default value is \$PN \$MAC -- Resync failed: \$ERR</p> <p><b>In the phone configuration file with XML(cfg.xml)</b>, enter a string in this format:  <pre>&lt;Log_Failure_Msg ua="na"&gt;\$PN \$MAC -- Resync failed: \$ERR&lt;/Log_Failure_Msg&gt;</pre> </p>

## Unique Profiles, Macro Expansion, and HTTP

In a deployment where each phone must be configured with distinct values for some parameters, such as `User_ID` or `Display_Name`, the service provider can create a unique profile for each deployed device and host those profiles on a provisioning server. Each phone, in turn, must be configured to resync to its own profile according to a predetermined profile naming convention.

The profile URL syntax can include identifying information that is specific to each phone, such as MAC address or serial number, by using the macro expansion of built-in variables. Macro expansion eliminates the need to specify these values in multiple locations within each profile.

A profile rule undergoes macro expansion before the rule is applied to the phone. The macro expansion controls a number of values, for example:

- `$MA` expands to the unit 12-digit MAC address (using lower case hex digits). For example, 000e08abcdef.
- `$SN` expands to the unit serial number. For example, 88012BA01234.

Other values can be macro expanded in this way, including all the general purpose parameters, `GPP_A` through `GPP_P`. An example of this process can be seen in [TFTP Resync, on page 34](#). Macro expansion is not limited to the URL file name, but can also be applied to any portion of the profile rule parameter. These parameters are referenced as `$A` through `$P`. For a complete list of variables that are available for macro expansion, see [Macro Expansion Variables, on page 69](#).

In this exercise, a profile specific to a phone is provisioned on a TFTP server.

### Provision a Specific IP Phone Profile on a TFTP Server

#### Procedure

- 
- Step 1** Obtain the MAC address of the phone from its product label. (The MAC address is the number, using numbers and lower-case hex digits, such as 000e08aabbcc).
  - Step 2** Move the new file in the virtual root directory of the TFTP server.
  - Step 3** Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).
  - Step 4** Select **Voice > Provisioning**.
  - Step 5** Click **Submit All Changes**. This causes an immediate reboot and resync.

When the next resync occurs, the phone retrieves the new file by expanding the `$MA` macro expression into its MAC address.

---

### HTTP GET Resync

HTTP provides a more reliable resync mechanism than TFTP because HTTP establishes a TCP connection and TFTP uses the less reliable UDP. In addition, HTTP servers offer improved filtering and logging features compared to TFTP servers.



On the client side, the phone does not require any special configuration setting on the server to be able to resync by using HTTP. The Profile\_Rule parameter syntax for using HTTP with the GET method is similar to the syntax that is used for TFTP. If a standard web browser can retrieve a profile from your HTTP server, the phone should be able to do so as well.

## Resync with HTTP GET

### Procedure

---

- Step 1** Install an HTTP server on the local PC or other accessible host.  
The open source Apache server can be downloaded from the internet.
- Step 2** Copy the `basic.txt` configuration profile (described in [TFTP Resync, on page 34](#)) onto the virtual root directory of the installed server.
- Step 3** To verify proper server installation and file access to `basic.txt`, access the profile with a web browser.
- Step 4** Modify the Profile\_Rule of the test phone to point to the HTTP server in place of the TFTP server, so as to download its profile periodically.  
For example, assuming the HTTP server is at 192.168.1.300, enter the following value:
- ```
<Profile_Rule>
http://192.168.1.200/basic.txt
</Profile_Rule>
```
- Step 5** Click **Submit All Changes**. This causes an immediate reboot and resync.
- Step 6** Observe the syslog messages that the phone sends. The periodic resyncs should now be obtaining the profile from the HTTP server.
- Step 7** In the HTTP server logs, observe how information that identifies the test phone appears in the log of user agents.  
This information should include the manufacturer, product name, current firmware version, and serial number.
- 

## Provisioning Through Cisco XML

For each of the phones, designated as xxxx here, you can provision through Cisco XML functions.

You can send an XML object to the phone by a SIP Notify packet or an HTTP Post to the CGI interface of the phone: `http://IPAddressPhone/CGI/Execute`.

The CP-xxxx-3PCC extends the Cisco XML feature to support provisioning via an XML object:

```
<CP-xxxx-3PCCExecute>
  <ExecuteItem URL=Resync:[profile-rule]/>
</CP-xxxx-3PCCExecute>
```

After the phone receives the XML object, it downloads the provisioning file from [profile-rule]. This rule uses macros to simplify the development of the XML services application.

## URL Resolution with Macro Expansion

Subdirectories with multiple profiles on the server provide a convenient method for managing a large number of deployed devices. The profile URL can contain:

- A provisioning server name or an explicit IP address. If the profile identifies the provisioning server by name, the phone performs a DNS lookup to resolve the name.
- A nonstandard server port that is specified in the URL by using the standard syntax `:port` following the server name.
- The subdirectory of the server virtual root directory where the profile is stored, specified by using standard URL notation and managed by macro expansion.

For example, the following Profile\_Rule requests the profile file (`$PN.cfg`), in the server subdirectory `/cisco/config`, from the TFTP server that is running on host `prov.telco.com` listening for a connection on port 6900:

```
<Profile_Rule>
tftp://prov.telco.com:6900/cisco/config/$PN.cfg
</Profile_Rule>
```

A profile for each phone can be identified in a general purpose parameter, with its value referred within a common profile rule by using macro expansion.

For example, assume `GPP_B` is defined as `Dj6Lmp23Q`.

The Profile\_Rule has the value:

```
tftp://prov.telco.com/cisco/$B/$MA.cfg
```

When the device resyncs and the macros are expanded, the phone with a MAC address of `000e08012345` requests the profile with the name that contains the device MAC address at the following URL:

```
tftp://prov.telco.com/cisco/Dj6Lmp23Q/000e08012345.cfg
```

## Resync a Device Automatically

A device can resync periodically to the provisioning server to ensure that any profile changes made on the server are propagated to the endpoint device (as opposed to sending an explicit resync request to the endpoint).

To cause the phone to periodically resync to a server, a configuration profile URL is defined by using the Profile\_Rule parameter, and a resync period is defined by using the Resync\_Periodic parameter.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

---

**Step 1** Select **Voice > Provisioning**.

- Step 2** Define the `Profile_Rule` parameter. This example assumes a TFTP server IP address of 192.168.1.200.
- Step 3** In the **Resync Periodic** field, enter a small value for testing, such as **30** seconds.
- Step 4** Click **Submit all Changes**.
- With the new parameter settings, the phone resyncs twice a minute to the configuration file that the URL specifies.
- Step 5** Observe the resulting messages in the syslog trace (as described in the [Use Syslog to Log Messages, on page 34](#) section).
- Step 6** Ensure that the **Resync On Reset** field is set to **Yes**.
- ```
<Resync_On_Reset>Yes</Resync_On_Reset>
```
- Step 7** Power cycle the phone to force it to resync to the provisioning server.
- If the resync operation fails for any reason, such as if the server is not responding, the unit waits (for the number of seconds configured in **Resync Error Retry Delay**) before it attempts to resync again. If **Resync Error Retry Delay** is zero, the phone does not try to resync after a failed resync attempt.
- Step 8** (Optional) Set the value of **Resync Error Retry Delay** field to a small number, such as **30**.
- ```
<Resync_Error_Retry_Delay>30</Resync_Error_Retry_Delay>
```
- Step 9** Disable the TFTP server, and observe the results in the syslog output.

## Profile Resync Parameters

The following table defines the function and usage of the profile resync parameters in the **Configuration Profile** section under the **Voice > Provisioning** tab in the phone web page. It also defines the syntax of the string that is added in the phone configuration file (cfg.xml) with XML code to configure a parameter.


Parameter	Description
Provision Enable	<p>Allows or denies configuration profile resync actions.</p> <ul style="list-style-type: none"> <li>• <b>In the phone configuration file (cfg.xml) with XML</b>, enter a string in this format:  <pre>&lt;Provision_Enable ua="na"&gt;Yes&lt;/Provision_Enable&gt;</pre> </li> <li>• <b>On the phone web page</b>, set this field to <b>Yes</b> to allow resync actions, or <b>No</b> to block resync actions.</li> </ul> <p>Default: Yes</p>

Parameter	Description
Resync On Reset	<p>Specifies whether the phone resynchronizes configurations with the provisioning server after power-up and after each upgrade attempt.</p> <ul style="list-style-type: none"> <li>• <b>In the phone configuration file (cfg.xml) with XML</b>, enter a string in this format:  <pre>&lt;Resync_On_Reset ua="na"&gt;Yes&lt;/Resync_On_Reset&gt;</pre> </li> <li>• <b>On the phone web page</b>, set this field to <b>Yes</b> to allow resync on power-up or reset, or <b>No</b> to block resync on power-up or reset.</li> </ul> <p>Default: Yes</p>
Resync Random Delay	<p>Prevents an overload of the provisioning server when a large number of devices power-on simultaneously and attempt initial configuration. This delay is effective only on the initial configuration attempt, following a device power-on or reset.</p> <p>The parameter is the maximum time interval that the device waits before making contact with the provisioning server. The actual delay is a pseudo-random number between 0 and this value.</p> <p>This parameter is in units of 20 seconds.</p> <p>The valid value ranges between 0 and 65535.</p> <ul style="list-style-type: none"> <li>• <b>In the phone configuration file (cfg.xml) with XML</b>, enter a string in this format:  <pre>&lt;Resync_Random_Delay ua="na"&gt;2&lt;/Resync_Random_Delay&gt;</pre> </li> <li>• <b>On the phone web page</b>, specify the number of the units (20 seconds) for the phone to delay resync after power-up or reset.</li> </ul> <p>The default value is 2 (40 seconds).</p>
Resync At (HHmm)	<p>The time (HHmm) that the phone resynchronizes with the provisioning server.</p> <p>The value for this field must be a four-digit number ranging from 0000 to 2400 to indicate the time in HHmm format. For example, 0959 indicates 09:59.</p> <ul style="list-style-type: none"> <li>• <b>In the phone configuration file (cfg.xml) with XML</b>, enter a string in this format:  <pre>&lt;Resync_At__HHmm_ ua="na"&gt;0959&lt;/Resync_At__HHmm_&gt;</pre> </li> <li>• <b>On the phone web page</b>, specify the time in HHMM format for the phone to start resync.</li> </ul> <p>The default value is empty. If the value is invalid, the parameter is ignored. If this parameter is set with a valid value, the <b>Resync Periodic</b> parameter is ignored.</p>

Parameter	Description
Resync At Random Delay	<p>Prevents an overload of the provisioning server when a large number of devices power on simultaneously.</p> <p>To avoid flooding resync requests to the server from multiple phones, the phone resynchronizes in the range between the hours and minutes, and the hours and minutes plus the random delay (hhmm, hhmm+random_delay). For example, if the random delay = (Resync At Random Delay + 30)/60minutes, the input value in seconds is converted to minutes, rounding up to the next minute to calculate the final random_delay interval.</p> <ul style="list-style-type: none"> <li>• <b>In the phone configuration file (cfg.xml) with XML</b>, enter a string in this format: <pre data-bbox="670 632 1437 657">&lt;Resync_At_Random_Delay ua="na"&gt;600&lt;/Resync_At_Random_Delay&gt;</pre> </li> <li>• <b>On the phone web page</b>, specify the time period in seconds.</li> </ul> <p>The valid value ranges between 600 and 65535.</p> <p>If the value is less than 600, the random delay interval is between 0 and 600.</p> <p>The default value is 600 seconds (10minutes).</p>
Resync Periodic	<p>The time interval between periodic resynchronization with the provisioning server. The associated resync timer is active only after the first successful sync with the server.</p> <p>The valid formats are as follows:</p> <ul style="list-style-type: none"> <li>• An integer <p>Example: An input of <b>3000</b> indicates that the next resync occurs in 3000 seconds.</p> </li> <li>• Multiple integers <p>Example: An input of <b>600 , 1200 , 300</b> indicates that the first resync occurs in 600 seconds, the second resync occurs in 1200 seconds after the first one, and the third resync occurs in 300 seconds after the second one.</p> </li> <li>• A time range <p>Example, an input of <b>2400+30</b> indicates that the next resync occurs in between 2400 and 2430 seconds after a successful resync.</p> </li> </ul> <ul style="list-style-type: none"> <li>• <b>In the phone configuration file (cfg.xml) with XML</b>, enter a string in this format: <pre data-bbox="670 1465 1271 1491">&lt;Resync_Periodic ua="na"&gt;3600&lt;/Resync_Periodic&gt;</pre> </li> <li>• <b>On the phone web page</b>, specify the time period in seconds.</li> </ul> <p>Set this parameter to zero to disable periodic resynchronization.</p> <p>The default value is 3600 seconds.</p>

Parameter	Description
Resync Error Retry Delay	<p>If a resync operation fails because the phone was unable to retrieve a profile from the server, or the downloaded file is corrupt, or an internal error occurs, the phone tries to resync again after a time specified in seconds.</p> <p>The valid formats are as follows:</p> <ul style="list-style-type: none"> <li>• An integer Example: An input of <b>300</b> indicates that the next retry for resync occurs in 300 seconds.</li> <li>• Multiple integers Example: An input of <b>600 , 1200 , 300</b> indicates that the first retry occurs in 600 seconds after the failure, the second retry occurs in 1200 seconds after the failure of the first retry, and the third retry occurs in 300 seconds after the failure of the second retry.</li> <li>• A time range Example, an input of <b>2400+30</b> indicates that the next retry occurs in between 2400 and 2430 seconds after a resync failure.</li> </ul> <p>If the delay is set to 0, the device does not try to resync again following a failed resync attempt.</p> <ul style="list-style-type: none"> <li>• <b>In the phone configuration file (cfg.xml) with XML</b>, enter a string in this format: <pre>&lt;Resync_Error_Retry_Delay ua="na"&gt;60,120,240,480,960,1920,3840,7680,15360,30720,61440,86400&lt;/Resync_Error_Retry_Delay&gt;</pre></li> <li>• <b>On the phone web page</b>, specify the time period in seconds.</li> </ul> <p>Default: 60,120,240,480,960,1920,3840,7680,15360,30720,61440,86400</p>
Forced Resync Delay	<p>Maximum delay (in seconds) the phone waits before performing a resynchronization. The device does not resync while one of its phone lines is active. Because a resync can take several seconds, it is desirable to wait until the device has been idle for an extended period before resynchronizing. This allows a user to make calls in succession without interruption.</p> <p>The device has a timer that begins counting down when all of its lines become idle. This parameter is the initial value of the counter. Resync events are delayed until this counter decrements to zero.</p> <p>The valid value ranges between 0 and 65535.</p> <ul style="list-style-type: none"> <li>• <b>In the phone configuration file (cfg.xml) with XML</b>, enter a string in this format: <pre>&lt;Forced_Resync_Delay ua="na"&gt;14400&lt;/Forced_Resync_Delay&gt;</pre></li> <li>• <b>On the phone web page</b>, specify the time period in seconds.</li> </ul> <p>The default value is 14,400seconds.</p>

Parameter	Description
Resync From SIP	<p>Controls requests for resync operations via a SIP NOTIFY event sent from the service provider proxy server to the phone. If enabled, the proxy can request a resync by sending a SIP NOTIFY message containing the Event: resync header to the device.</p> <ul style="list-style-type: none"> <li>• <b>In the phone configuration file (cfg.xml) with XML</b>, enter a string in this format: <pre>&lt;Resync_From_SIP ua="na"&gt;Yes&lt;/Resync_From_SIP&gt;</pre> </li> <li>• <b>On the phone web page</b>, select <b>Yes</b> to enable this feature, or <b>No</b> to disalbe it.</li> </ul> <p>Default: Yes</p>
Resync After Upgrade Attempt	<p>Enables or disables the resync operation after any upgrade occurs. If <b>Yes</b> is selected, sync is triggered after a firmware upgrade.</p> <ul style="list-style-type: none"> <li>• <b>In the phone configuration file (cfg.xml) with XML</b>, enter a string in this format: <pre>&lt;Resync_After_Upgrade_Attempt ua="na"&gt;Yes&lt;/Resync_After_Upgrade_Attempt&gt;</pre> </li> <li>• <b>On the phone web page</b>, select <b>Yes</b> to trigger resync after a firmware upgrade, or <b>No</b> to not resync.</li> </ul> <p>Default: Yes</p>
Resync Trigger 1 Resync Trigger 2	<p>If the logical equation in these parameters evaluates to FALSE, resync is not triggered even when <b>Resync On Reset</b> is set to <b>TRUE</b>. Only the resync via direct action URL and SIP notify ignores these resync triggers.</p> <p>The parameters can be programmed with a conditional expression that undergoes macro expansion. For the valid macro expansions, see <a href="#">Macro Expansion Variables, on page 69</a>.</p> <ul style="list-style-type: none"> <li>• <b>In the phone configuration file (cfg.xml) with XML</b>, enter a string in this format: <pre>&lt;Resync_Trigger_1 ua="na"&gt;\$UPGTMR gt 300 and \$PRVTMR ge 600&lt;/Resync_Trigger_1&gt; &lt;Resync_Trigger_2 ua="na"/&gt;</pre> </li> <li>• <b>On the phone web page</b>, specify the triggers.</li> </ul> <p>Default: Blank</p>

Parameter	Description
User Configurable Resync	<p>Allows a user to resync the phone from the phone screen menu. When set to <b>Yes</b>, a user can resync the phone configuration by entering the profile rule from the phone. When set to <b>No</b>, the <b>Profile rule</b> parameter isn't displayed on the phone screen menu. The <b>Profile rule</b> parameter is located under <b>Applications</b>  <b>&gt; Device administration</b>.</p> <ul style="list-style-type: none"> <li>• <b>In the phone configuration file (cfg.xml) with XML</b>, enter a string in this format:  <pre>&lt;User_Configurable_Resync ua="na"&gt;Yes&lt;/User_Configurable_Resync&gt;</pre> </li> <li>• <b>On the phone web page</b>, select <b>Yes</b> to show the <b>Profile rule</b> parameter on the phone menu, or select <b>No</b> to hide this parameter.</li> </ul> <p>Default: Yes</p>
Resync Fails On FNF	<p>A resync is typically considered unsuccessful if a requested profile is not received from the server. This parameter override this behavior. When set to <b>No</b>, the device accepts a <code>file-not-found</code> response from the server as a successful resync.</p> <ul style="list-style-type: none"> <li>• <b>In the phone configuration file (cfg.xml) with XML</b>, enter a string in this format:  <pre>&lt;Resync_Fails_On_FNF ua="na"&gt;Yes&lt;/Resync_Fails_On_FNF&gt;</pre> </li> <li>• <b>On the phone web page</b>, select <b>Yes</b> to take a <code>file-not-found</code> response as an unsuccessful resync, or select <b>No</b> to take a <code>file-not-found</code> response as a successful resync.</li> </ul> <p>Default: Yes</p>



Parameter	Description
Profile Authentication Type	<p>Specifies the credentials to use for profile account authentication. The available options are:</p> <ul style="list-style-type: none"> <li>• <b>Disabled:</b> Disables the profile account feature. When this feature is disabled, the <b>Profile account setup</b> menu doesn't display on the phone screen.</li> <li>• <b>Basic HTTP Authentication:</b> The HTTP login credentials are used to authenticate the profile account.</li> <li>• <b>XSI Authentication:</b> XSI login credentials or XSI SIP credentials are used to authenticate the profile account. The authentication credentials depend on the <b>XSI Authentication Type</b> for the phone: <ul style="list-style-type: none"> <li>• When the <b>XSI Authentication Type</b> for the phone is set to <b>Login Credentials</b>, the XSI login credentials are used.</li> <li>• When the <b>XSI Authentication Type</b> for the phone is set to <b>SIP Credentials</b>, the XSI SIP credentials are used.</li> </ul> </li> <li>• <b>In the phone configuration file (cfg.xml) with XML</b>, enter a string in this format: <pre>&lt;Profile_Authentication_Type ua="na"&gt;Basic Http Authentication&lt;/Profile_Authentication_Type&gt;</pre> </li> <li>• <b>On the phone web page</b>, select an option from the list for the phone to authenticate profile resync.</li> </ul> <p>Default: Basic HTTP Authentication</p>
Profile Rule Profile Rule B Profile Rule C Profile Rule D	<p>Each profile rule informs the phone of a source from which to obtain a profile (configuration file). During every resync operation, the phone applies all the profiles in sequence.</p> <p>If you are applying AES-256-CBC encryption to the configuration files, specify the encryption key with the <b>--key</b> keyword as follows:</p> <pre>[--key &lt;encryption key&gt;]</pre> <p>You can enclose the encryption key in double-quotes (") optionally.</p> <ul style="list-style-type: none"> <li>• <b>In the phone configuration file (cfg.xml) with XML</b>, enter a string in this format: <pre>&lt;Profile_Rule ua="na"&gt;/\$PSN.xml&lt;/Profile_Rule&gt; &lt;Profile_Rule_B ua="na"/&gt; &lt;Profile_Rule_C ua="na"/&gt; &lt;Profile_Rule_D ua="na"/&gt;</pre> </li> <li>• <b>On the phone web page</b>, specify the profile rule.</li> </ul> <p>Default: <b>/\$PSN.xml</b></p>
DHCP Option To Use	<p>DHCP options, delimited by commas, used to retrieve firmware and profiles.</p> <p>Default: 66,160,159,150,60,43,125</p>

Parameter	Description
DHCPv6 Option To Use	DHCP options, delimited by commas, used to retrieve firmware and profiles. Default: 17,160,159

## Set Up Your Phones for Activation Code Onboarding

If your network is configured for Activation Code Onboarding, you can set up new phones to register automatically in a secure way. You generate and provide each user with a unique 16-digit activation code. The user enters the activation code, and the phone automatically registers. This feature keeps your network secure because the phone can't register until the user enters a valid activation code.

Activation codes can be used only once, and have an expiry date. If a user enters an expired code, the phone displays `Invalid activation code` on the screen. If this happens, provide the user with a new code.

This feature is available in firmware release 11-2-3MSR1, BroadWorks Application Server Release 22.0 (patch AP.as.22.0.1123.ap368163 and its dependencies). However, you can change phones with older firmware to use this feature. To do this, use the following procedure.

### Before you begin

Ensure that you allow the `activation.webex.com` service through your firewall to support onboarding via activation code.

If you want to set up a proxy server for the onboarding, ensure that the proxy server is configured correctly. See [Set Up a Proxy Server, on page 132](#).

Access the phone web page. [Access the Phone Web Interface, on page 100](#)

### Procedure

- 
- Step 1** Reset the phone to the factory settings.
  - Step 2** Select **Voice > Provisioning > Configuration Profile**.
  - Step 3** Enter the profile rule in the **Profile Rule** field as described in the [Activation Code Provisioning Parameters, on page 48](#) table.
  - Step 4** (Optional) In the **Firmware Upgrade** section, enter the upgrade rule in the **Upgrade Rule** field as described in the [Activation Code Provisioning Parameters, on page 48](#) table.
  - Step 5** Submit All Changes.
- 

## Activation Code Provisioning Parameters

The following table defines the function and usage of the activation code parameters in the **Configuration Profile** section under the **Voice > Provisioning** tab in the phone web page. It also defines the syntax of the string that is added in the phone configuration file (`cfg.xml`) with XML code to configure a parameter.

Parameter	Description
Profile Rule Profile Rule B Profile Rule C Profile Rule D	<p>Remote configuration profile rules evaluated in sequence. Each resync operation can retrieve multiple files, potentially managed by different servers.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file (cfg.xml) with XML, enter a string in this format: <pre>&lt;Profile_Rule ua="na"&gt;gds://&lt;/Profile_Rule&gt;</pre> </li> <li>In the phone web interface, enter a string in this format: <pre>gds://</pre> </li> </ul> <p>Default: /\$PSN.xml</p>
Upgrade Rule	<p>Specifies the firmware upgrade script that defines upgrade conditions and associated firmware URLs. It uses the same syntax as Profile Rule.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file (cfg.xml) with XML, enter a string in this format: <pre>&lt;Upgrade_Rule ua="na"&gt;http://&lt;server ip address&gt;/ sip88xx.11-2-3MSR1-1.loads&lt;/Upgrade_Rule&gt;</pre> </li> <li>In the phone web interface, enter the upgrade rule: <pre>protocol://server[:port]/profile_pathname</pre> <p>For example:</p> <pre>tftp://192.168.1.5/image/sip88xx.11-2-3MSR1-1.loads</pre> </li> </ul> <p>If no protocol is specified, TFTP is assumed. If no server-name is specified, the host that requests the URL is used as the server name. If no port is specified, the default port is used (69 for TFTP, 80 for HTTP, or 443 for HTTPS).</p> <p>Default: Blank</p>

## Migrate Your Phone to Enterprise Phone Directly

You can now migrate your phone to enterprise phone easily in one step without using transition firmware load.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

- 
- Step 1** Select **Voice > Provisioning**.
- Step 2** In the **Upgrade Rule** field, set the Upgrade Rule parameter by entering a firmware upgrade script. For the syntax details, see that defines upgrade conditions and associated firmware URLs. It uses the same syntax as Profile Rule. Enter a script and use the following format to enter the upgrade rule:

```
<tftp|http|https>://<ipaddress>/image/<load name>
```

For example:

```
tftp://192.168.1.5/image/sip78xx.14-1-1MN-366.loads
```

**Step 3** Configure the **Transition Authorization Rule** parameter by entering a value to obtain and authorize the licence from the server.

You can also configure this parameter in the configuration file (cfg.xml) by entering a string in this format:

```
<Trans_Auth_Rule ua="na">http://10.74.51.81/prov/migration/E2312.lic</Trans_Auth_Rule>
```

**Step 4** In the **Transition Authorization Type** parameter, set the license type as **Classic**.

You can also configure this parameter in the configuration file (cfg.xml) by entering a string in this format:

```
<Trans_Auth_Type ua="na">Classic</Trans_Auth_Type>
```

**Step 5** Click **Submit All Changes**.

---

## Secure HTTPS Resync

These mechanisms are available on the phone for resyncing by using a secure communication process:

- Basic HTTPS Resync
- HTTPS with Client Certificate Authentication
- HTTPS Client Filtering and Dynamic Content

## Basic HTTPS Resync

HTTPS adds SSL to HTTP for remote provisioning so that the:

- The phone can authenticate the provisioning server.
- Provisioning server can authenticate the phone.
- Confidentiality of information exchanged between the phone and the provisioning server is ensured.

SSL generates and exchanges secret (symmetric) keys for each connection between the phone and the server, using public/private key pairs that are pre-installed in the phone and the provisioning server.

On the client side, the phone does not require any special configuration setting on the server to be able to resync using HTTPS. The Profile\_Rule parameter syntax for using HTTPS with the GET method is similar to the syntax that is used for HTTP or TFTP. If a standard web browser can retrieve a profile from a your HTTPS server, the phone should be able to do so as well.

In addition to installing a HTTPS server, a SSL server certificate that Cisco signs must be installed on the provisioning server. The devices cannot resync to a server that is using HTTPS unless the server supplies a Cisco-signed server certificate. Instructions for creating signed SSL Certificates for Voice products can be found at <https://supportforums.cisco.com/docs/DOC-9852>.

## Authenticate with Basic HTTPS Resync

### Procedure

- Step 1** Install an HTTPS server on a host whose IP address is known to the network DNS server through normal hostname translation.
- The open source Apache server can be configured to operate as an HTTPS server when installed with the open source `mod_ssl` package.
- Step 2** Generate a server Certificate Signing Request for the server. For this step, you might need to install the open source OpenSSL package or equivalent software. If using OpenSSL, the command to generate the basic CSR file is as follows:
- ```
openssl req -new -out provserver.csr
```
- This command generates a public/private key pair, which is saved in the `privkey.pem` file.
- Step 3** Submit the CSR file (`provserver.csr`) to Cisco for signing.
- A signed server certificate is returned (`provserver.cert`) along with a Sipura CA Client Root Certificate, `spacroot.cert`.
- See <https://supportforums.cisco.com/docs/DOC-9852> for more information
- Step 4** Store the signed server certificate, the private key pair file, and the client root certificate in the appropriate locations on the server.
- In the case of an Apache installation on Linux, these locations are typically as follows:
- ```
# Server Certificate:
SSLCertificateFile /etc/httpd/conf/provserver.cert
# Server Private Key:
SSLCertificateKeyFile /etc/httpd/conf/pivkey.pem
# Certificate Authority:
SSLCACertificateFile /etc/httpd/conf/spacroot.cert
```
- Step 5** Restart the server.
- Step 6** Copy the `basic.txt` configuration file (described in [TFTP Resync, on page 34](#)) onto the virtual root directory of the HTTPS server.
- Step 7** Verify proper server operation by downloading `basic.txt` from the HTTPS server by using a standard browser from the local PC.
- Step 8** Inspect the server certificate that the server supplies.
- The browser probably does not recognize the certificate as valid unless the browser has been pre-configured to accept Cisco as a root CA. However, the phones expect the certificate to be signed this way.
- Modify the `Profile_Rule` of the test device to contain a reference to the HTTPS server, for example:

```
<Profile_Rule>
https://my.server.com/basic.txt
</Profile_Rule>
```

This example assumes the name of the HTTPS server is `my.server.com`.

**Step 9** Click **Submit All Changes**.

**Step 10** Observe the syslog trace that the phone sends.

The syslog message should indicate that the resync obtained the profile from the HTTPS server.

**Step 11** (Optional) Use an Ethernet protocol analyzer on the phone subnet to verify that the packets are encrypted.

In this exercise, client certificate verification was not enabled. The connection between the phone and server is encrypted. However, the transfer is not secure because any client can connect to the server and request the file, given knowledge of the file name and directory location. For secure resync, the server must also authenticate the client, as demonstrated in the exercise described in [HTTPS with Client Certificate Authentication, on page 52](#).

## HTTPS with Client Certificate Authentication

In the factory default configuration, the server does not request an SSL client certificate from a client. Transfer of the profile is not secure because any client can connect to the server and request the profile. You can edit the configuration to enable client authentication; the server requires a client certificate to authenticate the phone before it accepts a connection request.

Because of this requirement, the resync operation cannot be independently tested by using a browser that lacks the proper credentials. The SSL key exchange within the HTTPS connection between the test phone and the server can be observed with the `ssldump` utility. The utility trace shows the interaction between client and server.

### Authenticate HTTPS with Client Certificate

#### Procedure

**Step 1** Enable client certificate authentication on the HTTPS server.

**Step 2** In Apache (v.2), set the following in the server configuration file:

```
SSLVerifyClient require
```

Also, ensure that the `spacroot.cert` has been stored as shown in the [Basic HTTPS Resync, on page 50](#) exercise.

**Step 3** Restart the HTTPS server and observe the syslog trace from the phone.

Each resync to the server now performs symmetric authentication, so that both the server certificate and the client certificate are verified before the profile is transferred.

**Step 4** Use `ssldump` to capture a resync connection between the phone and the HTTPS server.

If client certificate verification is properly enabled on the server, the `ssldump` trace shows the symmetric exchange of certificates (first server-to-client, then client-to-server) before the encrypted packets that contain the profile.

With client authentication enabled, only a phone with a MAC address that matches a valid client certificate can request the profile from the provisioning server. The server rejects a request from an ordinary browser or other unauthorized device.

## Configure a HTTPS Server for Client Filtering and Dynamic Content

If the HTTPS server is configured to require a client certificate, the information in the certificate identifies the resyncing phone and supplies it with the correct configuration information.

The HTTPS server makes the certificate information available to CGI scripts (or compiled CGI programs) that are invoked as part of the resync request. For the purpose of illustration, this exercise uses the open source Perl scripting language, and assumes that Apache (v.2) is used as the HTTPS server.

### Procedure

**Step 1** Install Perl on the host that is running the HTTPS server.

**Step 2** Generate the following Perl reflector script:

```
#!/usr/bin/perl -wT
use strict;
print "Content-Type: text/plain\n\n";
print "<flat-profile><GPP_D>";

print "OU=$ENV{'SSL_CLIENT_I_DN_OU'},\n";
print "L=$ENV{'SSL_CLIENT_I_DN_L'},\n";
print "S=$ENV{'SSL_CLIENT_I_DN_S'},\n";
print "</GPP_D></flat-profile>";
```

**Step 3** Save this file with the file name `reflect.pl`, with executable permission (`chmod 755` on Linux), in the CGI scripts directory of the HTTPS server.

**Step 4** Verify accessibility of CGI scripts on the server (that is, `/cgi-bin/...`).

**Step 5** Modify the `Profile_Rule` on the test device to resync to the reflector script, as in the following example:

```
https://prov.server.com/cgi-bin/reflect.pl?
```

**Step 6** Click **Submit All Changes**.

**Step 7** Observe the syslog trace to ensure a successful resync.

**Step 8** Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

**Step 9** Select **Voice > Provisioning**.

**Step 10** Verify that the `GPP_D` parameter contains the information that the script captured.

This information contains the product name, MAC address, and serial number if the test device carries a unique certificate from the manufacturer. The information contains generic strings if the unit was manufactured before firmware release 2.0.

A similar script can determine information about the resyncing device and then provide the device with appropriate configuration parameter values.

---

## HTTPS Certificates

The phone provides a reliable and secure provisioning strategy that is based on HTTPS requests from the device to the provisioning server. Both a server certificate and a client certificate are used to authenticate the phone to the server and the server to the phone.

In addition to Cisco issued certifications, the phone also accepts server certificates from a set of commonly used SSL certificate providers.

To use HTTPS with the phone, you must generate a Certificate Signing Request (CSR) and submit it to Cisco. The phone generates a certificate for installation on the provisioning server. The phone accepts the certificate when it seeks to establish an HTTPS connection with the provisioning server.

## HTTPS Methodology

HTTPS encrypts the communication between a client and a server, thus protecting the message contents from other network devices. The encryption method for the body of the communication between a client and a server is based on symmetric key cryptography. With symmetric key cryptography, a client and a server share a single secret key over a secure channel that is protected by Public/Private key encryption.

Messages encrypted by the secret key can only be decrypted by using the same key. HTTPS supports a wide range of symmetric encryption algorithms. The phone implements up to 256-bit symmetric encryption, using the American Encryption Standard (AES), in addition to 128-bit RC4.

HTTPS also provides for the authentication of a server and a client engaged in a secure transaction. This feature ensures that a provisioning server and an individual client cannot be spoofed by other devices on the network. This capability is essential in the context of remote endpoint provisioning.

Server and client authentication is performed by using public/private key encryption with a certificate that contains the public key. Text that is encrypted with a public key can be decrypted only by its corresponding private key (and vice versa). The phone supports the Rivest-Shamir-Adleman (RSA) algorithm for public/private key cryptography.

## SSL Server Certificate

Each secure provisioning server is issued a secure sockets layer (SSL) server certificate that Cisco signs directly. The firmware that runs on the phone recognizes only a Cisco certificate as valid. When a client connects to a server by using HTTPS, it rejects any server certificate that is not signed by Cisco.

This mechanism protects the service provider from unauthorized access to the phone, or any attempt to spoof the provisioning server. Without such protection, an attacker might be able to reprogram the phone, to gain configuration information, or to use a different VoIP service. Without the private key that corresponds to a valid server certificate, the attacker is unable to establish communication with a phone.



## Obtain a Server Certificate

### Procedure

---

- Step 1** Contact a Cisco support person who will work with you on the certificate process. If you are not working with a specific support person, email your request to [ciscosb-certadmin@cisco.com](mailto:ciscosb-certadmin@cisco.com).
- Step 2** Generate a private key that will be used in a CSR (Certificate Signing Request). This key is private and you do not need to provide this key to Cisco support. Use open source “openssl” to generate the key. For example:
- ```
openssl genrsa -out <file.key> 1024
```
- Step 3** Generate a CSR that contains fields that identify your organization and location. For example:
- ```
openssl req -new -key <file.key> -out <file.csr>
```
- You must have the following information:
- Subject field—Enter the Common Name (CN) that must be an FQDN (Fully Qualified Domain Name) syntax. During SSL authentication handshake, the phone verifies that the certificate it receives is from the machine that presented it.
  - Server hostname—For example, provserv.domain.com.
  - Email address—Enter an email address so that customer support can contact you if needed. This email address is visible in the CSR.
- Step 4** Email the CSR (in zip file format) to the Cisco support person or to [ciscosb-certadmin@cisco.com](mailto:ciscosb-certadmin@cisco.com). The certificate is signed by Cisco. Cisco sends the certificate to you to install on your system.
- 

## Client Certificate

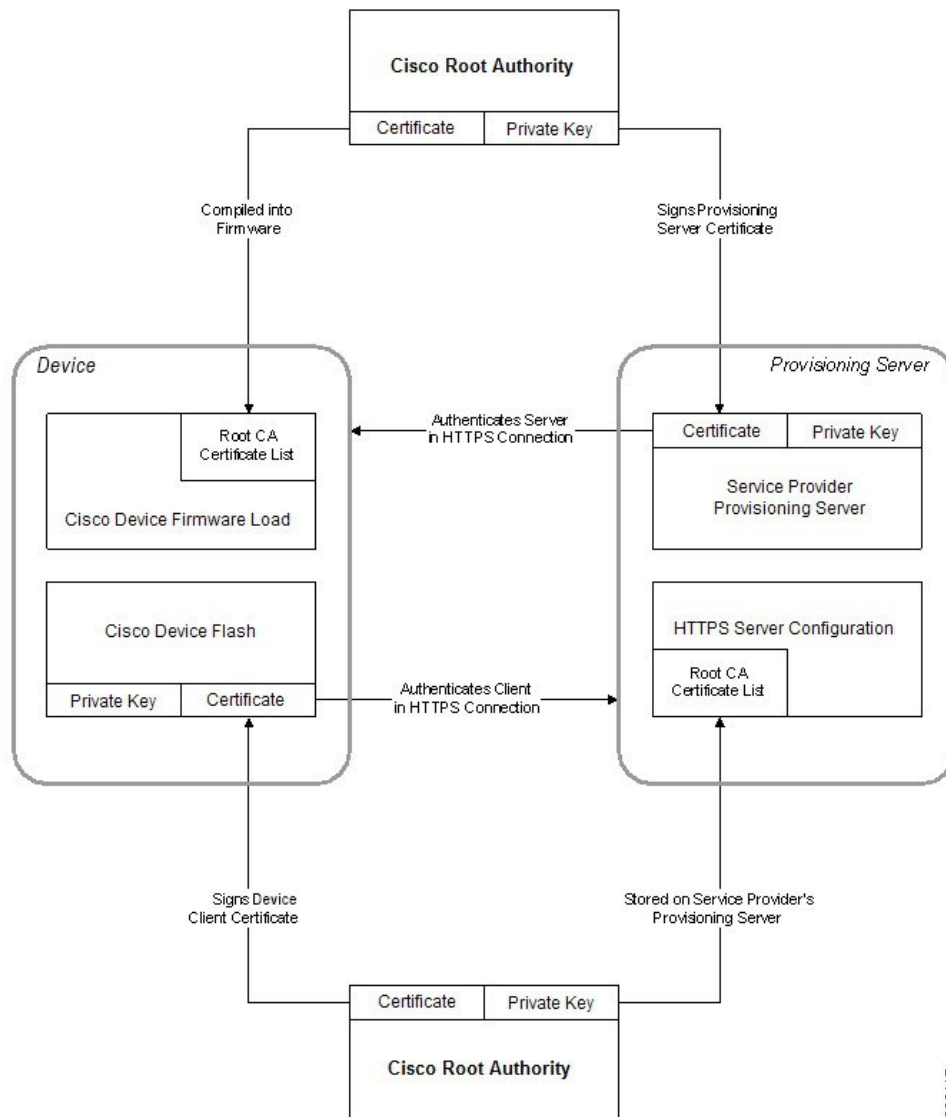
In addition to a direct attack on a phone, an attacker might attempt to contact a provisioning server through a standard web browser or another HTTPS client to obtain the configuration profile from the provisioning server. To prevent this kind of attack, each phone also carries a unique client certificate, signed by Cisco, that includes identifying information about each individual endpoint. A certificate authority root certificate that is capable of authenticating the device client certificate is given to each service provider. This authentication path allows the provisioning server to reject unauthorized requests for configuration profiles.

## Certificate Structure

The combination of a server certificate and a client certificate ensures secure communication between a remote phone and its provisioning server. The figure below illustrates the relationship and placement of certificates, public/private key pairs, and signing root authorities, among the Cisco client, the provisioning server, and the certification authority.

The upper half of the diagram shows the Provisioning Server Root Authority that is used to sign the individual provisioning server certificate. The corresponding root certificate is compiled into the firmware, which allows the phone to authenticate authorized provisioning servers.

Figure 6: Certificate Authority Flow



## Configure a Custom Certificate Authority

Digital certificates can be used to authenticate network devices and users on the network. They can be used to negotiate IPSec sessions between network nodes.

A third party uses a Certificate Authority certificate to validate and authenticate two or more nodes that are attempting to communicate. Each node has a public and private key. The public key encrypts data. The private key decrypts data. Because the nodes have obtained their certificates from the same source, they are assured of their respective identities.

The device can use digital certificates provided by a third-party Certificate Authority (CA) to authenticate IPSec connections.

The phones support a set of preloaded Root Certificate Authority embedded in the firmware:

- Cisco Small Business CA Certificate

- CyberTrust CA Certificate
- Verisign CA certificate
- Sipura Root CA Certificate
- Linksys Root CA Certificate

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

---

**Step 1** Select **Info > Status**.

**Step 2** Scroll to **Custom CA Status** and see the following fields:

- Custom CA Provisioning Status—Indicates the provisioning status.
    - Last provisioning succeeded on mm/dd/yyyy HH:MM:SS; or
    - Last provisioning failed on mm/dd/yyyy HH:MM:SS
  - Custom CA Info—Displays information about the custom CA.
    - Installed—Displays the “CN Value,” where “CN Value” is the value of the CN parameter for the Subject field in the first certificate.
    - Not Installed—Displays if no custom CA certificate is installed.
- 

## Profile Management

This section demonstrates the formation of configuration profiles in preparation for downloading. To explain the functionality, TFTP from a local PC is used as the resync method, although HTTP or HTTPS can be used as well.

### Compress an Open Profile with Gzip

A configuration profile in XML format can become quite large if the profile specifies all parameters individually. To reduce the load on the provisioning server, the phone supports compression of the XML file, by using the deflate compression format that the gzip utility (RFC 1951) supports.



---

**Note** Compression must precede encryption for the phone to recognize a compressed and encrypted XML profile.

---

For integration into customized back-end provisioning server solutions, the open source zlib compression library can be used in place of the standalone gzip utility to perform the profile compression. However, the phone expects the file to contain a valid gzip header.

### Procedure

---

**Step 1** Install gzip on the local PC.

**Step 2** Compress the `basic.txt` configuration profile (described in [TFTP Resync, on page 34](#)) by invoking gzip from the command line:

```
gzip basic.txt
```

This generates the deflated file `basic.txt.gz`.

**Step 3** Save the `basic.txt.gz` file in the TFTP server virtual root directory.

**Step 4** Modify the Profile\_Rule on the test device to resync to the deflated file in place of the original XML file, as shown in the following example:

```
tftp://192.168.1.200/basic.txt.gz
```

**Step 5** Click **Submit All Changes**.

**Step 6** Observe the syslog trace from the phone.

Upon resync, the phone downloads the new file and uses it to update its parameters.

---

## Encrypt a Profile with OpenSSL

A compressed or uncompressed profile can be encrypted (however, a file must be compressed before it is encrypted). Encryption is useful when the confidentiality of the profile information is of particular concern, such as when TFTP or HTTP is used for communication between the phone and the provisioning server.

The phone supports symmetric key encryption by using the 256-bit AES algorithm. This encryption can be performed by using the open source OpenSSL package.

### Procedure

---

**Step 1** Install OpenSSL on a local PC. This might require that the OpenSSL application be recompiled to enable AES.

**Step 2** Using the `basic.txt` configuration file (described in [TFTP Resync, on page 34](#)), generate an encrypted file with the following command:

```
>openssl enc -aes-256-cbc -k MyOwnSecret -in basic.txt -out basic.cfg
```

The compressed `basic.txt.gz` file that was created in [Compress an Open Profile with Gzip, on page 57](#) also can be used, because the XML profile can be both compressed and encrypted.

- Step 3** Store the encrypted `basic.cfg` file in the TFTP server virtual root directory.
- Step 4** Modify the `Profile_Rule` on the test device to resync to the encrypted file in place of the original XML file. The encryption key is made known to the phone with the following URL option:

```
[--key MyOwnSecret ] tftp://192.168.1.200/basic.cfg
```

- Step 5** Click **Submit All Changes**.
- Step 6** Observe the syslog trace from the phone.
- Upon resync, the phone downloads the new file and uses it to update its parameters.

---

## Create Partitioned Profiles

A phone downloads multiple separate profiles during each resync. This practice allows management of different kinds of profile information on separate servers and maintenance of common configuration parameter values that are separate from account specific values.

### Procedure

---

- Step 1** Create a new XML profile, `basic2.txt`, that specifies a value for a parameter that makes it distinct from the earlier exercises. For instance, to the `basic.txt` profile, add the following:

```
<GPP_B>ABCD</GPP_B>
```

- Step 2** Store the `basic2.txt` profile in the virtual root directory of the TFTP server.
- Step 3** Leave the first profile rule from the earlier exercises in the folder, but configure the second profile rule (`Profile_Rule_B`) to point to the new file:

```
<Profile_Rule_B>tftp://192.168.1.200/basic2.txt
</Profile_Rule_B>
```

- Step 4** Click **Submit All Changes**.
- The phone now resyncs to both the first and second profiles, in that order, whenever a resync operation is due.
- Step 5** Observe the syslog trace to confirm the expected behavior.
- 

## Set the Phone Privacy Header

A user privacy header in the SIP message sets user privacy needs from the trusted network.

You can set the user privacy header value for each line extension using an XML tag in the `config.xml` file.

The privacy header options are:

- Disabled (default)
- none—The user requests that a privacy service applies no privacy functions to this SIP message.
- header—The user needs a privacy service to obscure headers which cannot be purged of identifying information.
- session—The user requests that a privacy service provide anonymity for the sessions.
- user—The user requests a privacy level only by intermediaries.
- id—The user requests that the system substitute an id that doesn't reveal the IP address or host name.

### Procedure

---

- Step 1** Edit the phone `config.xml` file in a text or XML editor.
- Step 2** Insert the `<Privacy_Header_N_ua="na">Value</Privacy_Header_N_>` tag, where N is the line extension number (1–10), and use one of the following values.
- Default value: **Disabled**
  - **none**
  - **header**
  - **session**
  - **user**
  - **id**
- Step 3** (Optional) Provision any addition line extensions using the same tag with the required line extension number.
- Step 4** Save the changes to the `config.xml` file.
- 

## Renew the MIC Certificate

You can renew the Manufacture Installed Certificate (MIC) by a specified or default Secure Unique Device Identifier (SUDI) service. If the MIC certificate expires, the features that use SSL/TLS don't work.

### Before you begin

- Ensure that you allow the `sudirenewal.cisco.com` service (port 80) through your firewall to support the MIC certificate renewal.
- Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

---

- Step 1** Select **Voice > Provisioning**.

- Step 2** Under the **MIC Cert Settings** section, set the parameters as defined in [Parameters for MIC Certificate Renewal by SUDI Service, on page 61](#).
- Step 3** Click **Submit All Changes**.  
After the certificate renewal is completed successfully, the phone reboots.
- Step 4** (Optional) Check the latest status of the MIC certificate renewal under the **MIC Cert Refresh Status** section from **Info > Download Status**.
- Note** If you restore the phone to factory settings, the phone still uses the renewed certificate.

## Parameters for MIC Certificate Renewal by SUDI Service

The following table defines the function and usage of each parameter in the **MIC Cert Settings** section of the **Voice > Provisioning** tab.

*Table 5: Parameters for MIC Certificate Renewal by SUDI Service*

Parameter Name	Description and Default Value
MIC Cert Refresh Enable	<p>Controls whether to enable the Manufacture Installed Certificate (MIC) renewal by the default or specified Secure Unique Device Identifier (SUDI) service.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file (cfg.xml) with XML, enter a string in this format:  <pre>&lt;MIC_Cert_Refresh_Enable ua="na"&gt;Yes&lt;/MIC_Cert_Refresh_Enable&gt;</pre> </li> <li>In the phone web interface, select <b>Yes</b> or <b>No</b> to enable or disable the MIC certificate renewal.</li> </ul> <p>Valid values: Yes and No Default: No</p>

Parameter Name	Description and Default Value
MIC Cert Refresh Rule	<p>Enter the HTTP URL of the SUDI service that provides the renewed MIC certificate, for example,</p> <pre>http://sudirenewal.cisco.com/</pre> <p><b>Note</b> Don't change the URL. Only the default URL is supported for the MIC certificate renewal.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file (cfg.xml) with XML, enter a string in this format: <pre>&lt;MIC_Cert_Refresh_Rule ua="na"&gt;http://sudirenewal.cisco.com/&lt;/MIC_Cert_Refresh_Rule&gt;</pre> </li> <li>In the phone web interface, enter the HTTP URL to use.</li> </ul> <p>Allowed values: A valid URL not exceeding 1024 characters</p> <p>Default: <code>http://sudirenewal.cisco.com/</code></p>





## CHAPTER 5

# Provisioning Parameters

- [Provisioning Parameters Overview](#), on page 63
- [Configuration Profile Parameters](#), on page 63
- [Firmware Upgrade Parameters](#), on page 68
- [General Purpose Parameters](#), on page 69
- [Macro Expansion Variables](#), on page 69
- [Internal Error Codes](#), on page 72

## Provisioning Parameters Overview

This chapter describes the provisioning parameters that can be used in configuration profile scripts

## Configuration Profile Parameters

The following table defines the function and usage of each parameter in the **Configuration Profile Parameters** section under the **Provisioning** tab.

Parameter Name	Description and Default Value
Provision Enable	Controls all resync actions independently of firmware upgrade actions. Set to <b>Yes</b> to enable remote provisioning.  The default value is Yes.
Resync On Reset	Triggers a resync after every reboot except for reboots caused by parameter updates and firmware upgrades.  The default value is Yes.

Parameter Name	Description and Default Value
Resync Random Delay	<p>A random delay following the boot-up sequence before performing the reset, specified in seconds. In a pool of IP Telephony devices that are scheduled to simultaneously power up, this introduces a spread in the times at which each unit sends a resync request to the provisioning server. This feature can be useful in a large residential deployment, in the case of a regional power failure.</p> <p>The value for this field must be an integer ranging between 0 and 65535.</p> <p>The default value is 2.</p>
Resync At (HHmm)	<p>The time (HHmm) that the device resynchronizes with the provisioning server.</p> <p>The value for this field must be a four-digit number ranging from 0000 to 2400 to indicate the time in HHmm format. For example, 0959 indicates 09:59.</p> <p>The default value is empty. If the value is invalid, the parameter is ignored. If this parameter is set with a valid value, the Resync Periodic parameter is ignored.</p>
Resync At Random Delay	<p>Prevents an overload of the provisioning server when a large number of devices power-on simultaneously.</p> <p>To avoid flooding resync requests to the server from multiple phones, the phone resynchronizes in the range between the hours and minutes, and the hours and minutes plus the random delay (hhmm, hhmm+random_delay). For example, if the random delay = (Resync At Random Delay + 30)/60 minutes, the input value in seconds is converted to minutes, rounding up to the next minute to calculate the final random_delay interval.</p> <p>The valid value ranges between 600 and 65535.</p> <p>If the value is less than 600, the random delay interval is between 0 and 600.</p> <p>The default value is 600 seconds (10 minutes).</p>

Parameter Name	Description and Default Value
Resync Periodic	<p>The time interval between periodic resynchronizes with the provisioning server. The associated resync timer is active only after the first successful sync with the server.</p> <p>The valid formats are as follows:</p> <ul style="list-style-type: none"><li>• An integer Example: An input of <b>3000</b> indicates that the next resync occurs in 3000 seconds.</li><li>• Multiple integers Example: An input of <b>600 , 1200 , 300</b> indicates that the first resync occurs in 600 seconds, the second resync occurs in 1200 seconds after the first one, and the third resync occurs in 300 seconds after the second one.</li><li>• A time range Example, an input of <b>2400+30</b> indicates that the next resync occurs in between 2400 and 2430 seconds after a successful resync.</li></ul> <p>Set this parameter to zero to disable periodic resynchronization.</p> <p>The default value is 3600 seconds.</p>

Parameter Name	Description and Default Value
Resync Error Retry Delay	<p>If a resync operation fails because the IP Telephony device was unable to retrieve a profile from the server, or the downloaded file is corrupt, or an internal error occurs, the device tries to resync again after a time specified in seconds.</p> <p>The valid formats are as follows:</p> <ul style="list-style-type: none"> <li>• An integer Example: An input of <b>300</b> indicates that the next retry for resync occurs in 300 seconds.</li> <li>• Multiple integers Example: An input of <b>600 , 1200 , 300</b> indicates that the first retry occurs in 600 seconds after the failure, the second retry occurs in 1200 seconds after the failure of the first retry, and the third retry occurs in 300 seconds after the failure of the second retry.</li> <li>• A time range Example, an input of <b>2400+30</b> indicates that the next retry occurs in between 2400 and 2430 seconds after a resync failure.</li> </ul> <p>If the delay is set to 0, the device does not try to resync again following a failed resync attempt.</p>
Forced Resync Delay	<p>Maximum delay (in seconds) the phone waits before performing a resynchronization.</p> <p>The device does not resync while one of its phone lines is active. Because a resync can take several seconds, it is desirable to wait until the device has been idle for an extended period before resynchronizing. This allows a user to make calls in succession without interruption.</p> <p>The device has a timer that begins counting down when all of its lines become idle. This parameter is the initial value of the counter. Resync events are delayed until this counter decrements to zero.</p> <p>The valid value ranges between 0 and 65535.</p> <p>The default value is 14,400 seconds.</p>
Resync From SIP	<p>Enables a resync to be triggered via a SIP NOTIFY message.</p> <p>The default value is Yes.</p>

Parameter Name	Description and Default Value
Resync After Upgrade Attempt	Enables or disables the resync operation after any upgrade occurs. If Yes is selected, sync is triggered.  The default value is Yes.
Resync Trigger 1, Resync Trigger 2	Configurable resync trigger conditions. A resync is triggered when the logic equation in these parameters evaluates to TRUE.  The default value is (empty).
Resync Fails On FNF	A resync is considered unsuccessful if a requested profile is not received from the server. This can be overridden by this parameter. When it is set to <b>no</b> , the device accepts a <code>file-not-found</code> response from the server as a successful resync.  The default value is Yes.
Profile Rule Profile Rule B Profile Rule C Profile Rule D	Each profile rule informs the phone of a source from which to obtain a profile (configuration file). During every resync operation, the phone applies all the profiles in sequence.  Default: <code>/\$PSN.xml</code>  If you are applying AES-256-CBC encryption to the configuration files, specify the encryption key with the <code>--key</code> keyword as follows:  <code>[--key &lt;encryption key&gt;]</code>  You can enclose the encryption key in double-quotes (") optionally.
DHCP Option To Use	DHCP options, delimited by commas, used to retrieve firmware and profiles.  The default value is 66,160,159,150,60,43,125.
Log Request Msg	This parameter contains the message that is sent to the syslog server at the start of a resync attempt.  The default value is <code>\$PN \$MAC -Requesting % \$SCHEME://\$SERVIP:\$PORT\$PATH</code> .
Log Success Msg	The syslog message that is issued upon successful completion of a resync attempt.  The default value is <code>\$PN \$MAC -Successful Resync % \$SCHEME://\$SERVIP:\$PORT\$PATH -- \$ERR</code> .

Parameter Name	Description and Default Value
Log Failure Msg	The syslog message that is issued after a failed resync attempt.  The default value is \$PN \$MAC -- Resync failed: \$ERR.
User Configurable Resync	Allows a user to resync the phone from the IP phone screen.  The default value is Yes.

## Firmware Upgrade Parameters

The following table defines the function and usage of each parameter in the **Firmware Upgrade** section of the **Provisioning** tab.

Parameter Name	Description and Default Value
Upgrade Enable	Enables firmware upgrade operations independently of resync actions.  The default value is Yes.
Upgrade Error Retry Delay	The upgrade retry interval (in seconds) applied in case of upgrade failure. The device has a firmware upgrade error timer that activates after a failed firmware upgrade attempt. The timer is initialized with the value in this parameter. The next firmware upgrade attempt occurs when this timer counts down to zero.  The default value is 3600 seconds.
Upgrade Rule	A firmware upgrade script that defines upgrade conditions and associated firmware URLs. It uses the same syntax as Profile Rule.  Use the following format to enter the upgrade rule:  <tftp http https>://<ip address><:port>/<path>/<load name>  For example:  tftp://192.168.1.5/firmware/sip8832.11-2-3MPP-321.loads  If no protocol is specified, TFTP is assumed. If no server-name is specified, the host that requests the URL is used as the server name. If no port is specified, the default port is used (69 for TFTP, 80 for HTTP, or 443 for HTTPS).  The default value is blank.
Log Upgrade Request Msg	Syslog message issued at the start of a firmware upgrade attempt.  Default: \$PN \$MAC -- Requesting upgrade \$SCHEME://\$SERVIP:\$PORT\$PATH

Parameter Name	Description and Default Value
Log Upgrade Success Msg	Syslog message issued after a firmware upgrade attempt completes successfully.  The default value is \$PN \$MAC -- Successful upgrade \$SCHEME://\$SERVIP:\$PORT\$PATH -- \$ERR
Log Upgrade Failure Msg	Syslog message issued after a failed firmware upgrade attempt.  The default value is \$PN \$MAC -- Upgrade failed: \$ERR
Peer Firmware Sharing	Enables or disables the Peer Firmware Sharing feature. Select <b>Yes</b> or <b>No</b> to enable or to disable the feature.  Default: Yes
Peer Firmware Sharing Log Server	Indicates the IP address and the port to which the UDP message is sent.  For example: 10.98.76.123:514 where, 10.98.76.123 is the IP address and 514 is the port number.

## General Purpose Parameters

The following table defines the function and usage of each parameter in the **General Purpose Parameters** section of the **Provisioning** tab.

Parameter Name	Description and Default Value
GPP A - GPP P	The general purpose parameters GPP_* are used as free string registers when configuring the phones to interact with a particular provisioning server solution. They can be configured to contain diverse values, including the following: <ul style="list-style-type: none"> <li>• Encryption keys.</li> <li>• URLs.</li> <li>• Multistage provisioning status information.</li> <li>• Post request templates.</li> <li>• Parameter name alias maps.</li> <li>• Partial string values, eventually combined into complete parameter values.</li> </ul> <p>The default value is blank.</p>

## Macro Expansion Variables

Certain macro variables are recognized within the following provisioning parameters:

- Profile\_Rule
- Profile\_Rule\_\*
- Resync\_Trigger\_\*
- Upgrade\_Rule
- Log\_\*
- GPP\_\* (under specific conditions)

Within these parameters, syntax types, such as \$NAME or \$(NAME), are recognized and expanded.

Macro variable substrings can be specified with the notation \$(NAME:p) and \$(NAME:p:q), where p and q are non-negative integers (available in revision 2.0.11 and above). The resulting macro expansion is the substring starting at character offset p, with length q (or else till end-of-string if q is not specified). For example, if GPP\_A contains ABCDEF, then \$(A:2) expands to CDEF, and \$(A:2:3) expands to CDE.

An unrecognized name is not translated, and the \$NAME or \$(NAME) form remains unchanged in the parameter value after expansion.

Parameter Name	Description and Default Value
\$	The form \$\$ expands to a single \$ character.
A through P	Replaced by the contents of the general purpose parameters GPP_A through GPP_P.
SA through SD	Replaced by special purpose parameters GPP_SA through GPP_SD. These parameters hold keys or passwords used in provisioning.  <b>Note</b> \$SA through \$SD are recognized as arguments to the optional resync URL qualifier, --key.
MA	MAC address using lower case hex digits, for example, 000e08aabbcc.
MAU	MAC address using upper case hex digits, for example 000E08AABBCC.
MAC	MAC address using lower case hex digits, and colons to separate hex digit pairs. For example 00:0e:08:aa:bb:cc.
PN	
PSN	
SN	Serial Number string. for example 88012BA01234.
CCERT	SSL Client Certificate status: Installed or Not Installed.



Parameter Name	Description and Default Value
IP	IP address of the phone within its local subnet. For example 192.168.1.100.
EXTIP	External IP of the phone, as seen on the Internet. For example 66.43.16.52.
SWVER	Software version string. For example, <ul style="list-style-type: none"> <li>• For Firmware Release 11.3(1)SR1 and previous: sip8832.11-0-1MPP-312</li> <li>• For Firmware Release 11.3(2) and later: sip8832.11-3-2MPP0001-609</li> </ul>
HWVER	
PRVST	Provisioning State (a numeric string): -1 = explicit resync request 0 = power-up resync 1 = periodic resync 2 = resync failed, retry attempt
UPGST	Upgrade State (a numeric string): 1 = first upgrade attempt 2 = upgrade failed, retry attempt
UPGERR	Result message (ERR) of previous upgrade attempt; for example http_get failed.
PRVTMR	Seconds since last resync attempt.
UPGTMR	Seconds since last upgrade attempt.
REGTMR1	Seconds since Line 1 lost registration with SIP server.
REGTMR2	Seconds since Line 2 lost registration with SIP server.
UPGCOND	Legacy macro name.
SCHEME	File access scheme, one of TFTP, HTTP, or HTTPS, as obtained after parsing resync or upgrade URL.
SERV	Request target server host name, as obtained after parsing resync or upgrade URL.
SERVIP	Request target server IP address, as obtained after parsing resync or upgrade URL, possibly following DNS lookup.

Parameter Name	Description and Default Value
PORT	Request target UDP/TCP port, as obtained after parsing resync or upgrade URL.
PATH	Request target file path, as obtained after parsing resync or upgrade URL.
ERR	Result message of resync or upgrade attempt. Only useful in generating result syslog messages. The value is preserved in the UPGERR variable in the case of upgrade attempts.
UIDn	The contents of the Line n UserID configuration parameter.

## Internal Error Codes

The phone defines a number of internal error codes (X00–X99) to facilitate configuration in providing finer control over the behavior of the unit under certain error conditions.

Parameter Name	Description and Default Value
X00	Transport layer (or ICMP) error when sending a SIP request.
X20	SIP request times out while waiting for a response.
X40	General SIP protocol error (for example, unacceptable codec in SDP in 200 and ACK messages, or times out while waiting for ACK).
X60	Dialed number invalid according to given dial plan.



## CHAPTER 6

# Provisioning Formats

---

- [Configuration Profiles](#) , on page 73
- [Configuration Profile Formats](#), on page 73
- [Open Profile \(XML\) Compression and Encryption](#), on page 77
- [Application of a Profile to the Phone](#), on page 83
- [Provisioning Parameter Types](#), on page 84
- [Data Types](#), on page 90
- [Profile Updates and Firmware Upgrades](#), on page 93

## Configuration Profiles

The phone accepts configuration in an XML format.

The examples in this document use configuration profiles with an XML format (XML) syntax.

For detailed information about your phone, refer to the administration guide for your particular device. Each guide describes the parameters that can be configured through the administration web server.

## Configuration Profile Formats

The configuration profile defines the parameter values for the phone.

The configuration profile XML format uses standard XML authoring tools to compile the parameters and values.



---

**Note** Only the UTF-8 charset is supported. If you modify the profile in an editor, do not change the encoding format; otherwise, the phone cannot recognize the file.

---

Each phone has a different feature set and therefore, a different set of parameters.

### XML Format (XML) Profile

The open format profile is a text file with XML-like syntax in a hierarchy of elements, with element attributes and values. This format lets you use standard tools to create the configuration file. A configuration file in this

format can be sent from the provisioning server to the phone during a resync operation. The file can be sent without compilation as a binary object.

The phone can accept configuration formats that standard tools generate. This feature eases the development of back-end provisioning server software that generates configuration profiles from existing databases.

To protect confidential information in the configuration profile, the provisioning server delivers this type of file to the phone over a channel secured by TLS. Optionally, the file can be compressed by using the gzip deflate algorithm (RFC1951).

The file can be encrypted with one of these encryption methods:

- AES-256-CBC encryption
- RFC-8188 based HTTP content encryption with AES-128-GCM ciphering

### Example: Open Profile Format

```
<flat-profile>
<Resync_On_Reset> Yes </Resync_On_Reset>
<Resync_Periodic> 7200 </Resync_Periodic>
<Profile_Rule> tftp://prov.telco.com:6900/cisco/config/CP_xxxx_MPP.cfg</Profile_Rule>
</flat-profile>
```

The `<flat-profile>` element tag encloses all parameter elements that the phone recognizes.

## Configuration File Components

A configuration file can include these components:

- Element tags
- Attributes
- Parameters
- Formatting features
- XML comments

### Element Tag Properties

- The XML provisioning format and the Web UI allow the configuration of the same settings. The XML tag name and the field names in the Web UI are similar but vary due to XML element name restrictions. For example, underscores ( `_` ) instead of "  ".
- The phone recognizes elements with proper parameter names that are encapsulated in the special `<flat-profile>` element.
- Element names are enclosed in angle brackets.
- Most element names are similar to the field names in the administration web pages for the device, with the following modifications:

- Element names may not include spaces or special characters. To derive the element name from the administration web field name, substitute an underscore for every space or the special characters [ , ], ( , ), or /.

**Example:** The <Resync\_On\_Reset> element represents the **Resync On Reset** field.

- Each element name must be unique. In the administration web pages, the same fields can appear on multiple web pages, such as the Line, User, and Extension pages. Append [n] to the element name to indicate the number that is shown in the page tab.

**Example:** The <Dial\_Plan\_1\_> element represents the **Dial Plan** for Line 1.

- Each opening element tag must have a matching closing element tag. For example:

```
<flat-profile>
<Resync_On_Reset> Yes
  </Resync_On_Reset>
<Resync_Periodic> 7200
  </Resync_Periodic>
<Profile_Rule>tftp://prov.telco.com: 6900/cisco/config/CP_xxxx_MPP.cfg
  </Profile_Rule>
</flat-profile>
```

- Element tags are case-sensitive.
- Empty element tags are allowed and will be interpreted as configuring the value to be empty. Enter the opening element tag without a corresponding element tag, and insert a space and a forward slash before the closing angle bracket (>). In this example, Profile Rule B is empty:

```
<Profile_Rule_B />
```

- An empty element tag can be used to prevent the overwriting of any user-supplied values during a resync operation. In the following example, the user speed dial settings are unchanged:

```
<flat-profile>
<Speed_Dial_2_Name ua="rw"/>
<Speed_Dial_2_Number ua="rw"/>
<Speed_Dial_3_Name ua="rw"/>
<Speed_Dial_3_Number ua="rw"/>
<Speed_Dial_4_Name ua="rw"/>
<Speed_Dial_4_Number ua="rw"/>
<Speed_Dial_5_Name ua="rw"/>
<Speed_Dial_5_Number ua="rw"/>
<Speed_Dial_6_Name ua="rw"/>
<Speed_Dial_6_Number ua="rw"/>
<Speed_Dial_7_Name ua="rw"/>
<Speed_Dial_7_Number ua="rw"/>
<Speed_Dial_8_Name ua="rw"/>
<Speed_Dial_8_Number ua="rw"/>
<Speed_Dial_9_Name ua="rw"/>
<Speed_Dial_9_Number ua="rw"/>
</flat-profile>
```

- Use an empty value to set the corresponding parameter to an empty string. Enter an opening and closing element without any value between them. In the following example, the GPP\_A parameter is set to an empty string.

```
<flat-profile>
<GPP_A>
```

```
</GPP_A>
</flat-profile>
```

- Unrecognized element names are ignored.

## Parameter Properties

These properties apply to the parameters:

- Any parameters that are not specified by a profile are left unchanged in the phone.
- Unrecognized parameters are ignored.
- If the Open format profile contains multiple occurrences of the same parameter tag, the last such occurrence overrides any earlier ones. To avoid inadvertent override of configuration values for a parameter, we recommend that each profile specify at most one instance of a parameter.
- The last profile processed takes precedence. If multiple profiles specify the same configuration parameter, the value of the latter profile takes precedence.

## String Formats

These properties apply to the formatting of the strings:

- Comments are allowed through standard XML syntax.
 

```
<!-- My comment is typed here -->
```
- Leading and trailing white space is allowed for readability but is removed from the parameter value.
- New lines within a value are converted to spaces.
- An XML header of the form `<? ?>` is allowed, but the phone ignores it.
- To enter special characters, use basic XML character escapes, as shown in the following table.

Special Character	XML Escape Sequence
& (ampersand)	&amp;
< (less than)	&lt;
> (greater than)	&gt;
' (apostrophe)	&apos;
" (double quote)	&quot;

In the following example, character escapes are entered to represent the greater than and less than symbols that are required in a dial plan rule. This example defines an information hotline dial plan that sets the `<Dial_Plan_1_>` parameter (**Admin Login > advanced > Voice > Ext (n)**) equal to (S0 <:18005551212>).

```
<flat-profile>
<Dial_Plan_1_>
(S0 &lt;:18005551212&gt;)
</Dial_Plan_1_>
</flat-profile>
```

- Numeric character escapes, using decimal and hexadecimal values (s.a. `&#40;`; and `&#x2e;`), are translated.
- The phone firmware only supports ASCII characters.

## Open Profile (XML) Compression and Encryption

The Open configuration profile can be compressed to reduce the network load on the provisioning server. The profile can also be encrypted to protect confidential information. Compression is not required, but it must precede encryption.

### Open Profile Compression

The supported compression method is the gzip deflate algorithm (RFC1951). The gzip utility and the compression library that implements the same algorithm (zlib) are available from Internet sites.

To identify compression, the phone expects the compressed file to contain a gzip compatible header. Invocation of the gzip utility on the original Open profile generates the header. The phone inspects the downloaded file header to determine the file format.

For example, if `profile.xml` is a valid profile, the file `profile.xml.gz` is also accepted. Either of the following commands can generate this profile type:

- `>gzip profile.xml`  
Replaces original file with compressed file.
- `>cat profile.xml | gzip > profile.xml.gz`  
Leaves original file in place, produces new compressed file.

A tutorial on compression is provided in the [Compress an Open Profile with Gzip, on page 57](#) section.

### Open Profile Encryption

Symmetric key encryption can be used to encrypt an open configuration profile, whether the file is compressed or not. Compression, if applied, must be applied before encryption.

The provisioning server uses HTTPS to handle initial provisioning of the phone after deployment. Pre-encrypting configuration profiles offline allows the use of HTTP for resyncing profiles subsequently. This reduces the load on the HTTPS server in large-scale deployments.

The phone supports two methods of encryption for configuration files:

- AES-256-CBC encryption
- RFC 8188-based HTTP content encryption with AES-128-GCM ciphering

The key or Input Keying Material (IKM) must be preprovisioned into the unit at an earlier time. Bootstrap of the secret key can be accomplished securely by using HTTPS.

The configuration file name does not require a specific format, but a file name that ends with the `.cfg` extension normally indicates a configuration profile.

## AES-256-CBC Encryption

The phone supports AES-256-CBC encryption for configuration files.

The OpenSSL encryption tool, available for download from various Internet sites, can perform the encryption. Support for 256-bit AES encryption may require recompilation of the tool to enable the AES code. The firmware has been tested against version openssl-1.1.1d.

[Encrypt a Profile with OpenSSL, on page 58](#) provides a tutorial on encryption.

For an encrypted file, the profile expects the file to have the same format as generated by the following command:

```
# example encryption key = SecretPhrase1234
openssl enc -e -aes-256-cbc -k SecretPhrase1234 -in profile.xml -out profile.cfg
# analogous invocation for a compressed xml file
openssl enc -e -aes-256-cbc -k SecretPhrase1234 -in profile.xml.gz -out profile.cfg
```

A lowercase `-k` precedes the secret key, which can be any plain text phrase, and which is used to generate a random 64-bit salt. With the secret specified by the `-k` argument, the encryption tool derives a random 128-bit initial vector and the actual 256-bit encryption key.

When this form of encryption is used on a configuration profile, the phone must be informed of the secret key value to decrypt the file. This value is specified as a qualifier in the profile URL. The syntax is as follows, using an explicit URL:

```
[--key "SecretPhrase1234"] http://prov.telco.com/path/profile.cfg
```

This value is programmed by using one of the `Profile_Rule` parameters.

## Macro Expansion

Several provisioning parameters undergo macro expansion internally prior to being evaluated. This preevaluation step provides greater flexibility in controlling the phone resync and upgrade activities.

These parameter groups undergo macro expansion before evaluation:

- Resync\_Trigger\_\*
- Profile\_Rule\*
- Log\_xxx\_Msg
- Upgrade\_Rule

Under certain conditions, some general-purpose parameters (`GPP_*`) also undergo macro expansion, as explicitly indicated in [Optional Resync Arguments, on page 82](#).

During macro expansion, the contents of the named variables replace expressions of the form `$NAME` and `$(NAME)`. These variables include general-purpose parameters, several product identifiers, certain event timers, and provisioning state values. For a complete list, see [Macro Expansion Variables, on page 69](#).

In the following example, the expression `$(MAU)` is used to insert the MAC address 000E08012345.

The administrator enters: `$(MAU) config.cfg`



The resulting macro expansion for a device with MAC address 000E08012345 is:  
000E08012345config.cfg

If a macro name is not recognized, it remains unexpanded. For example, the name STRANGE is not recognized as a valid macro name, while MAU is recognized as a valid macro name.

The administrator enters: **\$STRANGE\$MAU.cfg**

The resulting macro expansion for a device with MAC address 000E08012345 is:  
\$STRANGE000E08012345.cfg

Macro expansion is not applied recursively. For example, \$\$MAU" expands into \$MAU" (the \$\$ is expanded), and does not result in the MAC address.

The contents of the special purpose parameters, GPP\_SA through GPP\_SD, are mapped to the macro expressions \$SA through \$SD. These parameters are only macro expanded as the argument of the **--key** , **--uid**, and **--pwd** options in a resync URL.

## Conditional Expressions

Conditional expressions can trigger resync events and select from alternate URLs for resync and upgrade operations.

Conditional expressions consist of a list of comparisons, separated by the **and** operator. All comparisons must be satisfied for the condition to be true.

Each comparison can relate to one of the following three types of literals:

- Integer values
- Software or hardware version numbers
- Doubled-quoted strings

### Version Numbers

The software version for Cisco IP Phones with Multiplatform Firmware uses this format (where *BN* is the Build Number):

- For Firmware Release 11.3(1)SR1 and previous: *sipyyyy.11-0-1MPP-376*  
where *yyyy* indicates the phone model or phone series; *11* is the major version; *0* is the minor version; *1MPP* is the micro version; and *376* is the build number.
- For Firmware Release 11.3(2) and later: *sipyyyy.11-3-2MPP0001-609*  
where *yyyy* indicates the phone model or phone series; *11* is the major version; *3* is the minor version; *2MPP0001* is the micro version; and *609* is the build number.

The comparing string must use the same format. Otherwise, a format parsing error results.

When comparing the software version, the major version, minor version, and micro version are compared in sequence, and the leftmost digits take precedence over the latter ones. When version numbers are identical, the build number is compared.

### Examples of Valid Version Number

- For Firmware Release 11.3(1)SR1 and previous:

```
sip8832.11-0-1MPP-312
```

- For Firmware Release 11.3(2) and later:

```
sip8832.11-3-2MPP0001-609
```

## Comparison

- For Firmware Release 11.3(1)SR1 and previous:

```
sipyyyy.11-3-1MPP-110 > sipyyy.11-2-3MPP-256
```

- For Firmware Release 11.3(2) and later:

```
sipyyyy.11-3-2MPP0002-256 > sipyyy.11-3-2MPP0001-609
```

Quoted strings can be compared for equality or inequality. Integers and version numbers can also be compared arithmetically. The comparison operators can be expressed as symbols or as acronyms. Acronyms are convenient for expressing the condition in an Open format profile.

Operator	Alternate Syntax	Description	Applicable to Integer and Version Operands	Applicable to Quoted String Operands
=	eq	equal to	Yes	Yes
!=	ne	not equal to	Yes	Yes
<	lt	less than	Yes	No
<=	le	less than or equal to	Yes	No
>	gt	greater than	Yes	No
>=	ge	greater than or equal to	Yes	No
AND		and	Yes	Yes

It is important to enclose macro variables in double quotes where a string literal is expected. Don't do so where a number or version number is expected.

When used in the context of the Profile\_Rule\* and Upgrade\_Rule parameters, conditional expressions must be enclosed within the syntax “(expr)?” as in this upgrade rule example. Remember to replace *BN* with the build number of your firmware load to upgrade to.

- For Firmware Release 11.3(1)SR1 and previous

```
($SWVER ne sip8832.11-0-0MPP-256)? http://ps.tell.com/sw/sip8832.11-0-0MPP-BN.loads
```

- For Firmware Release 11.3(2) and later

```
($SWVER ne sip8832.11-3-2MPP0001-609)?  
http://ps.tell.com/sw/sip8832xx.11-3-2MPP0001-BN.loads
```

Do not use the preceding syntax with parentheses to configure the Resync\_Trigger\_\* parameters.

## URL Syntax

Use the Standard URL syntax to specify how to retrieve configuration files and firmware loads in Profile\_Rule\* and Upgrade\_Rule parameters, respectively. The syntax is as follows:

```
[ scheme:// ] [ server [:port]] filepath
```

Where **scheme** is one of these values:

- tftp
- http
- https

If **scheme** is omitted, tftp is assumed. The server can be a DNS-recognized hostname or a numeric IP address. The port is the destination UDP or TCP port number. The filepath must begin with the root directory (/); it must be an absolute path.

If **server** is missing, the tftp server specified through DHCP (option 66) is used.




---

**Note** For upgrade rules, the server must be specified.

---

If **port** is missing, the standard port for the specified scheme is used. Tftp uses UDP port 69, http uses TCP port 80, https uses TCP port 443.

A filepath must be present. It need not necessarily refer to a static file, but can indicate dynamic content obtained through CGI.

Macro expansion applies within URLs. The following are examples of valid URLs:

```
/$MA.cfg
/cisco/cfg.xml
192.168.1.130/profiles/init.cfg
tftp://prov.call.com/cpe/cisco$MA.cfg
http://neptune.speak.net:8080/prov/$D/$E.cfg
https://secure.me.com/profile?Linksys
```

```
/$MA.cfg
/cisco/cfg.xml
192.168.1.130/profiles/init.cfg
tftp://prov.call.com/cpe/cisco$MA.cfg
```

When using DHCP option 66, the empty syntax is not supported by upgrade rules. It is only applicable for Profile Rule\*.

## RFC 8188-Based HTTP Content Encryption

The phone supports RFC 8188-based HTTP content encryption with AES-128-GCM ciphering for configuration files. With this encryption method, any entity can read the HTTP message headers. However, only the entities that know the Input Keying Material (IKM) can read the payload. When the phone is provisioned with the IKM, the phone and the provisioning server can exchange configuration files securely, while allowing third-party network elements to use the message headers for analytic and monitoring purposes.

The XML configuration parameter **IKM\_HTTP\_Encrypt\_Content** holds the IKM on the phone. For security reasons, this parameter is not accessible on the phone administration web page. It is also not visible

in the phone's configuration file, which you can access from the phone's IP address or from the phone's configuration reports sent to the provisioning server.

If you want to use the RFC 8188-based encryption, ensure the following:

- Provision the phone with the IKM by specifying the IKM with the XML parameter **IKM\_HTTP\_Encrypt\_Content** in the configuration file that is sent from the provisioning server to the phone.
- If this encryption is applied to the configuration files sent from the provisioning server to the phone, ensure that the *Content-Encoding* HTTP header in the configuration file has "aes128gcm".

In the absence of this header, the AES-256-CBC method is given precedence. The phone applies AES-256-CBC decryption if a AES-256-CBC key is present in a profile rule, regardless of IKM.

- If you want the phone to apply this encryption to the configuration reports that it sends to the provisioning server, ensure that there is no AES-256-CBC key specified in the report rule.

## Optional Resync Arguments

Optional arguments, **key**, **uid**, and **pwd**, can precede the URLs entered in Profile\_Rule\* parameters, collectively enclosed by square brackets.

### key

The **--key** option tells the phone that the configuration file that it receives from the provisioning server is encrypted with AES-256-CBC encryption, unless the *Content-Encoding* header in the file indicates "aes128gcm" encryption. The key itself is specified as a string following the term **--key**. The key can be enclosed in double-quotes (") optionally. The phone uses the key to decrypt the configuration file.

### Usage Examples

```
[--key VerySecretValue]
[--key "my secret phrase"]
[--key a37d2fb9055c1d04883a0745eb0917a4]
```

The bracketed optional arguments are macro expanded. Special purpose parameters, GPP\_SA through GPP\_SD, are macro expanded into macro variables, \$SA through \$SD, only when they are used as key option arguments. See these examples:

```
[--key $SC]
[--key "$SD"]
```

In Open format profiles, the argument to **--key** must be the same as the argument to the **-k** option that is given to **openssl**.

### uid and pwd

The **uid** and **pwd** options can be used to specify the userID and password that will be sent in response to HTTP Basic and Digest authentication challenges when the specified URL is requested. The bracketed optional arguments are macro expanded. Special purpose parameters, GPP\_SA through GPP\_SD, are macro expanded into macro variables, \$SA through \$SD, only when they are used as key option arguments. See these examples:

```
GPP_SA = MyUserID  
GPP_SB = MySecretPassword
```

```
 [--uid $SA --pwd $SB] https://provisioning_server_url/path_to_your_config/your_config.xml
```

would then expand to:

```
 [--uid MyUserID --pwdMySecretPassword]  
 https://provisioning_server_url/path_to_your_config/your_config.xml
```

## Application of a Profile to the Phone

After you create an XML configuration script, it must be passed to the phone for application. To apply the configuration, you can either download the configuration file to the phone from a TFTP, HTTP, or HTTPS server using a web browser or by using cURL command line utility.

### Download the Configuration File to the Phone from a TFTP Server

Complete these steps to download the configuration file to a TFTP server application on your PC.

#### Procedure

- 
- Step 1** Connect your PC to the phone LAN.
  - Step 2** Run a TFTP server application on the PC and ensure that the configuration file is available in the TFTP root directory.
  - Step 3** In a web browser, enter the phone LAN IP address, the IP address of the computer, the filename, and the login credentials. Use this format:

```
http://<WAN_IP_Address>/admin/resync?tftp://<PC_IP_Address>/<file_name>&xuser=admin&xpassword=<password>
```

Example:

```
http://192.168.15.1/admin/resync?tftp://192.168.15.100/my_config.xml&xuser=admin&xpassword=admin
```

---

### Download the Configuration File to the Phone with cURL

Complete these steps to download the configuration to the phone by using cURL. This command-line tool is used to transfer data with a URL syntax. To download cURL, visit:

<https://curl.haxx.se/download.html>



---

**Note** We recommend that you do not use cURL to post the configuration to the phone because the username and password might get captured while using cURL.

---

## Procedure

---

**Step 1** Connect your PC to the LAN port of the phone.

**Step 2** Download the configuration file to the phone by entering the following cURL command:

```
curl -d @my_config.xml  
"http://192.168.15.1/admin/config.xml&xuser=admin&xpassword=admin"
```

---

# Provisioning Parameter Types

This section describes the provisioning parameters broadly organized according to function:

These provisioning parameter types exist:

- General Purpose
- Enables
- Triggers
- Configurable Schedules
- Profile Rules
- Upgrade Rule

## General Purpose Parameters

The general-purpose parameters GPP\_\* (**Admin Login > advanced > Voice > Provisioning**) are used as free string registers when configuring the phone to interact with a particular provisioning server solution. The GPP\_\* parameters are empty by default. They can be configured to contain diverse values, including the following:

- Encryption keys
- URLs
- Multistage provisioning status information.
- Post request templates
- Parameter name alias maps
- Partial string values, eventually combined into complete parameter values.

The GPP\_\* parameters are available for macro expansion within other provisioning parameters. For this purpose, single-letter uppercase macro names (A through P) suffice to identify the contents of GPP\_A through GPP\_P. Also, the two-letter uppercase macro names SA through SD identify GPP\_SA through GPP\_SD as a special case when used as arguments of the following URL options:

**key**, **uid**, and **pwd**

These parameters can be used as variables in provisioning and upgrade rules. They are referenced by prefixing the variable name with a '\$' character, such as \$GPP\_A.

## Use General Purpose Parameters

For example, if GPP\_A contains the string ABC, and GPP\_B contains 123, the expression \$A\$B macro expands into ABC123.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

- 
- |               |                                                          |
|---------------|----------------------------------------------------------|
| <b>Step 1</b> | Select <b>Voice &gt; Provisioning</b> .                  |
| <b>Step 2</b> | Scroll to the <b>General Purpose Parameters</b> section. |
| <b>Step 3</b> | Enter valid values in the fields, GPP A through GPP P.   |
| <b>Step 4</b> | Click <b>Submit All Changes</b> .                        |
- 

## Enable Parameters

The Provision\_Enable and Upgrade\_Enable parameters control all profile resync and firmware upgrade operations. These parameters control resyncs and upgrades independently of each other. These parameters also control resync and upgrade URL commands that are issued through the administration web server. Both of these parameters are set to **Yes** by default.

The Resync\_From\_SIP parameter controls requests for resync operations. A SIP NOTIFY event is sent from the service provider proxy server to the phone. If enabled, the proxy can request a resync. To do so, the proxy sends a SIP NOTIFY message that contains the Event: resync header to the device.

The device challenges the request with a 401 response (authorization refused for used credentials). The device expects an authenticated subsequent request before it honors the resync request from the proxy. The Event: reboot\_now and Event: restart\_now headers perform cold and warm restarts, respectively, which are also challenged.

The two remaining enables are Resync\_On\_Reset and Resync\_After\_Upgrade\_Attempt. These parameters determine whether the device performs a resync operation after power-up software reboots and after each upgrade attempt.

When Resync\_On\_Reset is enabled, the device introduces a random delay that follows the boot-up sequence before the reset is performed. The delay is a random time up to the value that the Resync\_Random\_Delay (in seconds) specifies. In a pool of phones that power up simultaneously, this delay spreads out the start times of the resync requests from each unit. This feature can be useful in a large residential deployment, in the case of a regional power failure.

## Triggers

The phone allows you to resync at specific intervals or at a specific time.

## Resync at Specific Intervals

The phone is designed to resync with the provisioning server periodically. The resync interval is configured in Resync\_Periodic (seconds). If this value is left empty, the device does not resync periodically.

The resync typically takes place when the voice lines are idle. If a voice line is active when a resync is due, the phone delays the resync procedure until the line becomes idle again. A resync can cause configuration parameter values to change.

A resync operation can fail because the phone is unable to retrieve a profile from the server, the downloaded file is corrupt, or an internal error occurred. The device tries to resync again after a time that is specified in Resync\_Error\_Retry\_Delay (seconds). If Resync\_Error\_Retry\_Delay is set to 0, the device does not try to resync again after a failed resync attempt.

If an upgrade fails, a retry is performed after Upgrade\_Error\_Retry\_Delay seconds.

Two configurable parameters are available to conditionally trigger a resync: Resync\_Trigger\_1 and Resync\_Trigger\_2. Each parameter can be programmed with a conditional expression that undergoes macro expansion. When the resync interval expires (time for the next resync) the triggers, if set, will prevent resync unless one or more triggers evaluates to true.

The following example condition triggers a resync. In the example, the last phone upgrade attempt has elapsed more than 5 minutes (300 seconds), and at least 10 minutes (600 seconds) have elapsed since the last resync attempt.

```
$UPGTMR gt 300 and $PRVTMR ge 600
```

## Resync at a Specific Time

The Resync\_At parameter allows the phone to resync at a specific time. This parameter uses the 24-hour format (hhmm) to specify the time.

The Resync\_At\_Random\_Delay parameter allows the phone to resync at an unspecified delay in time. This parameter uses a positive integer format to specify the time.

Flooding the server with resync requests from multiple phones that are set to resync at the same time should be avoided. To do so, the phone triggers the resync up to 10 minutes after the specified time.

For example, if you set the resync time to 1000 (10 a.m.), the phone triggers the resync anytime between 10:00 a.m. and 10:10 a.m.

By default, this feature is disabled. If the Resync\_At parameter is provisioned, the Resync\_Periodic parameter is ignored.

## Configurable Schedules

You can configure schedules for periodic resyncs, and you can specify the retry intervals for resync and upgrade failures by using these provisioning parameters:

- Resync\_Periodic
- Resync\_Error\_Retry\_Delay
- Upgrade\_Error\_Retry\_Delay

Each parameter accepts a single delay value (seconds). The new extended syntax allows for a comma-separated list of consecutive delay elements. The last element in the sequence is implicitly repeated forever.



Optionally, you can use a plus sign to specify another numeric value that appends a random extra delay.

### Example 1

In this example, the phone periodically resyncs every 2 hours. If a resync failure occurs, the device retries at these intervals: 30 minutes, 1 hour, 2 hours, 4 hours. The device continues to try at 4-hour intervals until it resyncs successfully.

```
Resync_Periodic=7200  
Resync_Error_Retry_Delay=1800,3600,7200,14400
```

### Example 2

In this example, the device periodically resyncs every hour (plus an extra random delay of up to 10 minutes). In the case of a resync failure, the device retries at these intervals: 30 minutes (plus up to 5 minutes), 1 hour (plus up to 10 minutes), 2 hours (plus up to 15 minutes). The device continues to try at 2-hour intervals (plus up to 15 minutes) until it successfully resyncs.

```
Resync_Periodic=3600+600  
Resync_Error_Retry_Delay=1800+300,3600+600,7200+900
```

### Example 3

In this example, if a remote upgrade attempt fails, the device retries the upgrade in 30 minutes, then again after one more hour, then in two hours. If the upgrade still fails, the device retries every four to five hours until the upgrade succeeds.

```
Upgrade_Error_Retry_Delay = 1800,3600,7200,14400+3600
```

## Profile Rules

The phone provides multiple remote configuration profile parameters (Profile\_Rule\*). Thus, each resync operation can retrieve multiple files that different servers manage.

In the simplest scenario, the device resyncs periodically to a single profile on a central server, which updates all pertinent internal parameters. Alternatively, the profile can be split between different files. One file is common for all the phones in a deployment. A separate, unique file is provided for each account. Encryption keys and certificate information can be supplied by still another profile, stored on a separate server.

Whenever a resync operation is due, the phone evaluates the four Profile\_Rule\* parameters in sequence:

1. Profile\_Rule
2. Profile\_Rule\_B
3. Profile\_Rule\_C
4. Profile\_Rule\_D

Each evaluation can result in a profile retrieval from a remote provisioning server, with a possible update of some number of internal parameters. If an evaluation fails, the resync sequence is interrupted, and is retried again from the beginning specified by the Resync\_Error\_Retry\_Delay parameter (seconds). If all evaluations

succeed, the device waits for the second specified by the Resync\_Periodic parameter and then performs another resync.

The contents of each Profile\_Rule\* parameter consist of a set of alternatives. The alternatives are separated by the | (pipe) character. Each alternative consists of a conditional expression, an assignment expression, a profile URL, and any associated URL options. All these components are optional within each alternative. The following are the valid combinations, and the order in which they must appear, if present:

```
[ conditional-expr ] [ assignment-expr ] [[ options ] URL ]
```

Within each Profile\_Rule\* parameter, all alternatives except the last one must provide a conditional expression. This expression is evaluated and is processed as follows:

1. Conditions are evaluated from left to right, until one is found that evaluates as true (or until one alternative is found with no conditional expression).
2. Any accompanying assignment expression is evaluated, if present.
3. If a URL is specified as part of that alternative, an attempt is made to download the profile that is located at the specified URL. The system attempts to update the internal parameters accordingly.

If all alternatives have conditional expressions and none evaluates to true (or if the whole profile rule is empty), the entire Profile\_Rule\* parameter is skipped. The next profile rule parameter in the sequence is evaluated.

### Example 1

This example resyncs unconditionally to the profile at the specified URL, and performs an HTTP GET request to the remote provisioning server:

```
http://remote.server.com/cisco/$MA.cfg
```

### Example 2

In this example, the device resyncs to two different URLs, depending on the registration state of Line 1. In case of lost registration, the device performs an HTTP POST to a CGI script. The device sends the contents of the macro expanded GPP\_A, which may provide additional information on the device state:

```
($PRVTMR ge 600)? http://p.tel.com/has-reg.cfg  
| [--post a] http://p.tel.com/lost-reg?
```

### Example 3

In this example, the device resyncs to the same server. The device provides additional information if a certificate is not installed in the unit (for legacy pre-2.0 units):

```
("$CCERT" eq "Installed")? https://p.tel.com/config?  
| https://p.tel.com/config?cisco$MAU
```

**Example 4**

In this example, Line 1 is disabled until GPP\_A is set equal to Provisioned through the first URL. Afterwards, it resyncs to the second URL:

```
("SA" ne "Provisioned")? (Line_Enable_1_ = "No");! https://p.tel.com/init-prov
| https://p.tel.com/configs
```

**Example 5**

In this example, the profile that the server returns is assumed to contain XML element tags. These tags must be remapped to proper parameter names by the aliases map stored in GPP\_B:

```
[--alias b] https://p.tel.com/account/$PN$MA.xml
```

A resync is typically considered unsuccessful if a requested profile is not received from the server. The Resync\_Fails\_On\_FNF parameter can override this default behavior. If Resync\_Fails\_On\_FNF is set to No, the device accepts a file-not-found response from the server as a successful resync. The default value for Resync\_Fails\_On\_FNF is Yes.

## Upgrade Rule

Upgrade rule is to tell the device to activate to a new load and from where to get the load, if necessary. If the load is already on the device, it will not try to get the load. So, validity of the load location does not matter when the desired load is in the inactive partition.

The Upgrade\_Rule specifies a firmware load which, if different from the current load, will be downloaded and applied unless limited by a conditional expression or Upgrade\_Enable is set to **No**.

The phone provides one configurable remote upgrade parameter, Upgrade\_Rule. This parameter accepts syntax similar to the profile rule parameters. URL options are not supported for upgrades, but conditional expressions and assignment expressions can be used. If conditional expressions are used, the parameter can be populated with multiple alternatives, separated by the | character. The syntax for each alternative is as follows:

```
[ conditional-expr ] [ assignment-expr ] URL
```

As in the case of Profile\_Rule\* parameters, the Upgrade\_Rule parameter evaluates each alternative until a conditional expression is satisfied or an alternative has no conditional expression. The accompanying assignment expression is evaluated, if specified. Then, an upgrade to the specified URL is attempted.

If the Upgrade\_Rule contains a URL without a conditional expression, the device upgrades to the firmware image that the URL specifies. After macro expansion and evaluation of the rule, the device does not reattempt to upgrade until the rule is modified or the effective combination of scheme + server + port + filepath is changed.

To attempt a firmware upgrade, the device disables audio at the start of the procedure and reboots at the end of the procedure. The device automatically begins an upgrade that is driven by the contents of Upgrade\_Rule only if all voice lines are currently inactive.

For example,

In this example, the Upgrade\_Rule upgrades the firmware to the image that is stored at the indicated URL.

This example directs the unit to load one of two images, based on the contents of a general-purpose parameter, GPP\_F.

The device can enforce a downgrade limit regarding firmware revision number, which can be a useful customization option. If a valid firmware revision number is configured in the Downgrade\_Rev\_Limit parameter, the device rejects upgrade attempts for firmware versions earlier than the specified limit.

## Data Types

These data types are used with configuration profile parameters:

- {a,b,c,...}—A choice among a, b, c, ...
- Bool—Boolean value of either “yes” or “no.”
- CadScript—A miniscript that specifies the cadence parameters of a signal. Up to 127 characters.

Syntax:  $S_1[;S_2]$ , where:

- $S_i=D_i(\text{on}_{i,1}/\text{off}_{i,1}[\text{on}_{i,2}/\text{off}_{i,2}[\text{on}_{i,3}/\text{off}_{i,3}[\text{on}_{i,4}/\text{off}_{i,4}[\text{on}_{i,5}/\text{off}_{i,5}[\text{on}_{i,6}/\text{off}_{i,6}]]]])$  and is known as a section.
- $\text{on}_{i,j}$  and  $\text{off}_{i,j}$  are the on/off duration in seconds of a *segment*.  $i = 1$  or  $2$ , and  $j = 1$  to  $6$ .
- $D_i$  is the total duration of the section in seconds.

All durations can have up to three decimal places to provide 1 ms resolution. The wildcard character “\*” stands for infinite duration. The segments within a section are played in order and repeated until the total duration is played.

Example 1:

```
60 (2/4)

Number of Cadence Sections = 1
Cadence Section 1: Section Length = 60 s
Number of Segments = 1
Segment 1: On=2s, Off=4s

Total Ring Length = 60s
```

Example 2—Distinctive ring (short,short,short,long):

```
60 (.2/.2,.2/.2,.2/.2,1/4)

Number of Cadence Sections = 1
Cadence Section 1: Section Length = 60s
Number of Segments = 4
Segment 1: On=0.2s, Off=0.2s
Segment 2: On=0.2s, Off=0.2s
Segment 3: On=0.2s, Off=0.2s
Segment 4: On=1.0s, Off=4.0s

Total Ring Length = 60s
```

- DialPlanScript—Scripting syntax that is used to specify Line 1 and Line 2 dial plans.

- **Float<n>**—A floating point value with up to n decimal places.
- **FQDN**—Fully Qualified Domain Name. It can contain up to 63 characters. Examples are as follows:
  - sip.Cisco.com:5060 or 109.12.14.12:12345
  - sip.Cisco.com or 109.12.14.12
- **FreqScript**—A miniscript that specifies the frequency and level parameters of a tone. Contains up to 127 characters.

Syntax: F<sub>1</sub>@L<sub>1</sub>[,F<sub>2</sub>@L<sub>2</sub>[,F<sub>3</sub>@L<sub>3</sub>[,F<sub>4</sub>@L<sub>4</sub>[,F<sub>5</sub>@L<sub>5</sub>[,F<sub>6</sub>@L<sub>6</sub>]]]]], where:

- F<sub>1</sub>–F<sub>6</sub> are frequency in Hz (unsigned integers only).
- L<sub>1</sub>–L<sub>6</sub> are corresponding levels in dBm (with up to one decimal place).

White spaces before and after the comma are allowed but not recommended.

Example 1—Call Waiting Tone:

```
440@-10

Number of Frequencies = 1
Frequency 1 = 440 Hz at -10 dBm
```

Example 2—Dial Tone:

```
350@-19,440@-19

Number of Frequencies = 2
Frequency 1 = 350 Hz at -19 dBm
Frequency 2 = 440 Hz at -19 dBm
```

- **IP**—Valid IPv4 Address in the form of x.x.x.x, where x is between 0 and 255. Example: 10.1.2.100.
- **UserID**—User ID as it appears in a URL; up to 63 characters.
- **Phone**—A phone number string, such as 14081234567, \*69, \*72, 345678; or a generic URL, such as, 1234@10.10.10.100:5068 or jsmith@Cisco.com. The string can contain up to 39 characters.
- **PhTmpl**—A phone number template. Each template may contain one or more patterns that are separated by a comma (.). White space at the beginning of each pattern is ignored. “?” and “\*” represent wildcard characters. To represent literally, use %xx. For example, %2a represents \*. The template can contain up to 39 characters. Examples: “1408\*, 1510\*”, “1408123????, 555?1.”.
- **Port**—TCP/UDP Port number (0-65535). It can be specified in decimal or hex format.
- **ProvisioningRuleSyntax**—Scripting syntax that is used to define configuration resync and firmware upgrade rules.
- **PwrLevel**—Power level expressed in dBm with one decimal place, such as -13.5 or 1.5 (dBm).
- **RscTmpl**—A template of SIP Response Status Code, such as “404, 5\*”, “61?”, “407, 408, 487, 481”. It can contain up to 39 characters.
- **Sig<n>**—Signed n-bit value. It can be specified in decimal or hex format. A “-” sign must precede negative values. A + sign before positive values is optional.

- **Star Codes**—Activation code for a supplementary service, such as \*69. The code can contain up to 7 characters.
- **Str<n>**—A generic string with up to n nonreserved characters.
- **Time<n>**—Time duration in seconds, with up to n decimal places. Extra specified decimal places are ignored.
- **ToneScript**—A miniscript that specifies the frequency, level, and cadence parameters of a call progress tone. Script may contain up to 127 characters.

Syntax: FreqScript;Z<sub>1</sub>[:Z<sub>2</sub>].

The section Z<sub>1</sub> is similar to the S<sub>1</sub> section in a CadScript, except that each on/off segment is followed by a frequency components parameter: Z<sub>1</sub> = D<sub>1</sub>(on<sub>i,1</sub>/off<sub>i,1</sub>/f<sub>i,1</sub>[,on<sub>i,2</sub>/off<sub>i,2</sub>/f<sub>i,2</sub> [,on<sub>i,3</sub>/off<sub>i,3</sub>/f<sub>i,3</sub> [,on<sub>i,4</sub>/off<sub>i,4</sub>/f<sub>i,4</sub> [,on<sub>i,5</sub>/off<sub>i,5</sub>/f<sub>i,5</sub> [,on<sub>i,6</sub>/off<sub>i,6</sub>/f<sub>i,6</sub>]]]])) where:

- $f_{i,j} = n_1[+n_2]+n_3[+n_4[+n_5[+n_6]]]]]$ .
- $1 < n_k < 6$  specifies the frequency components in the FreqScript that are used in that segment.

If more than one frequency component is used in a segment, the components are summed together.

**Example 1—Dial tone:**

```
350@-19,440@-19;10(*0/1+2)

Number of Frequencies = 2
Frequency 1 = 350 Hz at -19 dBm
Frequency 2 = 440 Hz at -19 dBm
Number of Cadence Sections = 1
Cadence Section 1: Section Length = 10 s
Number of Segments = 1
Segment 1: On=forever, with Frequencies 1 and 2

Total Tone Length = 10s
```

**Example 2—Stutter tone:**

```
350@-19,440@-19;2(.1/.1/1+2);10(*0/1+2)

Number of Frequencies = 2
Frequency 1 = 350 Hz at -19 dBm
Frequency 2 = 440 Hz at -19 dBm
Number of Cadence Sections = 2
Cadence Section 1: Section Length = 2s
Number of Segments = 1
Segment 1: On=0.1s, Off=0.1s with Frequencies 1 and 2
Cadence Section 2: Section Length = 10s
Number of Segments = 1
Segment 1: On=forever, with Frequencies 1 and 2

Total Tone Length = 12s
```

- **Uns<n>**—Unsigned n-bit value, where n = 8, 16, or 32. It can be specified in decimal or hex format, such as 12 or 0x18, as long as the value can fit into n bits.



**Note** Keep these under consideration:

- <Par Name> represents a configuration parameter name. In a profile, the corresponding tag is formed by replacing the space with an underscore “\_”, such as **Par\_Name**.
- An empty default value field implies an empty string <“”>.
- The phone continues to use the last configured values for tags that are not present in a given profile.
- Templates are compared in the order given. The first, *not the closest*, match is selected. The parameter name must match exactly.
- If more than one definition for a parameter is given in a profile, the last such definition in the file is the one that takes effect in the phone.
- A parameter specification with an empty parameter value forces the parameter back to its default value. To specify an empty string instead, use the empty string "" as the parameter value.

## Profile Updates and Firmware Upgrades

The phone supports secure remote provisioning (configuration) and firmware upgrades. An unprovisioned phone can receive an encrypted profile targeted for that device. The phone does not require an explicit key due to a secure first-time provisioning mechanism that uses SSL functionality.

User intervention is not required to either start or complete a profile update, or firmware upgrade, or if intermediate upgrades are required to reach a future upgrade state from an older release. A profile resync is only attempted when the phone is idle, because a resync can trigger a software reboot and disconnect a call.

General-purpose parameters manage the provisioning process. Each phone can be configured to periodically contact a normal provisioning server (NPS). Communication with the NPS does not require the use of a secure protocol because the updated profile is encrypted by a shared secret key. The NPS can be a standard TFTP, HTTP, or HTTPS server with client certificates.

The administrator can upgrade, reboot, restart, or resync phones by using the phone web user interface. The administrator can also perform these tasks by using a SIP notify message.

Configuration profiles are generated by using common, open-source tools that integrate with service provider provisioning systems.

## Allow Profile Updates

Profile updates can be allowed at specified intervals. Updated profiles are sent from a server to the phone by using TFTP, HTTP, or HTTPS.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

---

**Step 1** Select **Voice > Provisioning**.

- Step 2** In the **Configuration Profile** section, choose **Yes** from the **Provision Enable** parameter.
- You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:
- ```
<Provision_Enable ua="na">Yes</Provision_Enable>
```
- Default: Yes
- Step 3** Set the parameters as described in the [Profile Resync Parameters, on page 41](#) table.
- Step 4** Click **Submit All Changes**.

## Allow and Configure Firmware Upgrades

Firmware updates can be allowed at specified intervals. Updated firmware is sent from a server to the phone by using TFTP or HTTP. Security is less of an issue with a firmware upgrade, because firmware does not contain personal information.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

- Step 1** Select **Voice > Provisioning**.
- Step 2** In the **Firmware Upgrade** section, choose **Yes** from the **Upgrade Enable** parameter.
- You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:
- ```
<Upgrade_Enable ua="na">Yes</Upgrade_Enable>
```
- Options: Yes and No
- Default: Yes
- Step 3** Set the **Upgrade Error Retry Delay** parameter in seconds.
- The upgrade retry interval (in seconds) applied in case of upgrade failure. The device has a firmware upgrade error timer that activates after a failed firmware upgrade attempt. The timer is initialized with the value in this parameter. The next firmware upgrade attempt occurs when this timer counts down to zero.
- You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:
- ```
<Upgrade_Error_Retry_Delay ua="na">3600</Upgrade_Error_Retry_Delay>
```
- Default: 3600
- :
- ```
<tftp|http|https>://<ip address>/image/<load name>
```



- Step 4** Set the **Upgrade Rule** parameter by entering a firmware upgrade script that defines upgrade conditions and associated firmware URLs. It uses the same syntax as Profile Rule. Enter a script and use the following format to enter the upgrade rule:

```
<tftp|http|https>://<ipaddress>/image/<load name>
```

For example:

```
tftp://192.168.1.5/image/sip88xx.11-0-0MPP-BN.loads
```

```
tftp://192.168.1.5/image/sip78xx.11-0-1MPP-BN.loads
```

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<Upgrade_Rule ua="na">http://10.74.10.205:6970/sip8845_65.0104-MPP-9875dev.loads  
</Upgrade_Rule>
```

- Step 5** Click **Submit All Changes**.
- 

## Upgrade Firmware by TFTP, HTTP, or HTTPS

The phone supports firmware upgrade by TFTP, HTTP, or HTTPS.



- Note** Downgrades to earlier releases may not be available for all devices. For more information, see the release notes for your phone and firmware version.
- 

### Before you begin

The firmware load file must be downloaded to an accessible server.

### Procedure

---

- Step 1** Copy the folder to a TFTP, HTTP, or HTTPS download directory.
- Step 2** Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).
- Step 3** Select **Voice > Provisioning**.
- Step 4** Click **Submit All Changes**.
- 

## Upgrade Firmware With a Browser Command

An upgrade command entered into the browser address bar can be used to upgrade firmware on a phone. The phone updates only when it is idle. The update is attempted automatically after the call is complete.

### Procedure

---

To upgrade the phone with a URL in a web browser, enter this command:

```
http://<phone_ip>/admin/upgrade?<schema>://<serv_ip[:port]>/filepath
```

---



## PART II

# Cisco IP Phone Configuration

- [Access Control Configuration, on page 99](#)
- [Third-Party Call Control Setup, on page 105](#)
- [Cisco IP Phone Security, on page 113](#)
- [Phone Features and Setup, on page 139](#)
- [Phone Information and Display Configuration, on page 227](#)
- [Call Features Configuration, on page 237](#)
- [Audio Configuration, on page 283](#)
- [Voicemail Configuration, on page 293](#)
- [Corporate and Personal Directory Setup, on page 297](#)





## CHAPTER 7

# Access Control Configuration

---

- [Access Control](#), on page 99
- [Administrator and User Accounts](#), on page 99
- [User Access Attribute](#), on page 100
- [Access the Phone Web Interface](#), on page 100
- [Control Access to the Phone Settings](#), on page 101
- [Bypass the Set Password Screen](#), on page 104

## Access Control

If the <Phone-UI-User-Mode> parameter is enabled, the phone GUI honors the user access attribute of the relevant parameters when the GUI presents a menu item.

For menu entries that are associated with a single configuration parameter:

- Provisioning the parameter with “ua=na” (“ua” stands for “user access”) attribute makes the entry disappear.
- Provisioning the parameter with “ua=ro” attribute makes the entry read-only and non-editable.

For menu entries that are associated with multiple configuration parameters:

- Provisioning all concerned parameters with “ua=na” attribute makes the entries disappear.

## Administrator and User Accounts

The Cisco IP Phone firmware provides specific administrator and user accounts. These accounts provide specific login privileges. The administrator account name is **admin**; the user account name is **user**. These account names cannot be changed.

The **admin** account gives the service provider or Value-added Reseller (VAR) configuration access to the Cisco IP phone. The **user** account gives limited and configurable control to the device end user.

The **user** and **admin** accounts can be password protected independently. If the service provider sets an administrator account password, you are prompted for it when you click **Admin Login**. If the password does not yet exist, the screen refreshes and displays the administration parameters. No default passwords are assigned to either the administrator or the user account. Only the administrator account can assign or change passwords.

The administrator account can view and modify all web profile parameters, including web parameters, that are available to the user login. The Cisco IP Phone system administrator can further restrict the parameters that a user account can view and modify through use of a provisioning profile.

Configuration parameters that are available to the user account are configurable on the Cisco IP Phone. User access to the phone web user interface can be disabled.

## User Access Attribute

The user access (**ua**) attribute controls may be used to change access by the User account. If the **ua** attribute is not specified, the existing user access setting is retained. This attribute does not affect access by the Admin account.

The **ua** attribute, if present, must have one of the following values:

- na—No access
- ro—Read-only
- rw—Read and write
- y—Preserve value

The **y** value must be used together with **na**, **ro**, or **rw**.

The following example illustrates the **ua** attribute. Notice in the last line that the **ua** attribute is updated to **rw**, and the station name field (**Travel Agent 1**) is preserved. If **y** is not included, **Travel Agent 1** is overwritten:

```
<flat-profile>
  <SIP_TOS_DiffServ_Value_1_ ua="na"/>
  <Dial_Plan_1_ ua="ro"/>
  <Dial_Plan_2_ ua="rw"/>
  <Station_Name ua="rw" preserve-value="y">Travel Agent 1</Station_Name></flat-profile>
```

Double quotes must enclose the value of the **ua** option.

## Access the Phone Web Interface

The phone firmware provides mechanisms for restricting end-user access to some parameters. The firmware provides specific privileges for sign-in to an **Admin** account or a **User** account. Each can be independently password-protected.

- Admin account—Allows the full access to all administration web server parameters
- User account—Allows the access to a subset of the administration web server parameters

If your service provider has disabled access to the configuration utility, contact the service provider before proceeding.

### Procedure

- 
- Step 1** Ensure that the computer can communicate with the phone. No VPN in use.

- Step 2** Start a web browser.
- Step 3** Enter the IP address of the phone in your web browser address bar.
- User Access: **http://<ip address>**
  - Admin Access: **http://<ip address>/admin/advanced**
  - Admin Access: **http://<ip address>**, click **Admin Login** and click **advanced**
- For example, `http://10.64.84.147/admin`
- Step 4** Enter the password when prompted.
- 

## Control Access to the Phone Settings

You can configure the phone to allow or block access to the configuration parameters on the phone web page or the phone screen. The parameters for access control allow you to:

- Indicate which configuration parameters are available to the user account when creating the configuration.
- Enable or disable the access to the administration web server.
- Enable or disable user access to the phone screen menus.
- Bypass the **Set password** screen for the user.
- Restrict the Internet domains that the phone accesses for resync, upgrades, or SIP registration for Line 1.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code. To configure each parameter, see the syntax of the string in [Access Control Parameters, on page 101](#).

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

---

- Step 1** Click **Voice > System**.
- Step 2** In the **System Configuration** section, configure the parameters as defined in the [Access Control Parameters, on page 101](#) table.
- Step 3** Click **Submit All Changes** to apply the changes.
- 


## Access Control Parameters

The following table defines the function and usage of the access control parameters in the **System Configuration** section under the **Voice > System** tab in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file (cfg.xml) with XML code to configure a parameter.

Table 6: Access Control Parameters

Parameter Name	Description and Default Value
Enable Web Server	<p>Enables or disables access to the phone web interface. Set this parameter to <b>Yes</b> to allow users or administrators to access the phone web interface. Otherwise, set it to <b>No</b>. When set to <b>No</b>, the phone web interface isn't accessible.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;Enable_Web_Server ua="na"&gt;Yes&lt;/Enable_Web_Server&gt;</pre> </li> <li>In the phone web interface, set to <b>Yes</b> to allow the access.</li> </ul> <p>Allowed values: Yes No Default: Yes.</p>
Enable Web Admin Access	<p>Allows or blocks the access to the phone administration pages: <b>http://&lt;phone_IP&gt;/admin</b></p> <p>When set to <b>No</b>, the web page for administrator is inaccessible. Only the web page for user is accessible.</p> <p><b>Note</b> If you want to allow the access to the administration web page again after the access is blocked, you need to perform a factory reset from the phone.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;Enable_Web_Admin_Access ua="na"&gt;Yes&lt;/Enable_Web_Admin_Access&gt;</pre> </li> <li>In the phone web interface, set this parameter to <b>Yes</b> to allow the access. Otherwise, set it to <b>No</b>.</li> </ul> <p>Allowed values: Yes No Default: Yes</p>
Admin Password	<p>Allows you to set or change the password for accessing the phone administration web pages.</p> <p>The Admin Password parameter is only available on the phone administration web page.</p> <p>A valid password must contain 4 to 127 characters from three out of the four types: capital letter, small letter, number, and special character.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;Admin_Password ua="na"&gt;P0ssw0rd_tes89&lt;/Admin_Password&gt;</pre> </li> <li>In the phone web interface, enter the password for administrator access.</li> </ul> <p>Default: Empty</p>



Parameter Name	Description and Default Value
User Password	<p>Allows you or the phone user to set or change the password for accessing the phone web interfaces and the menus on the phone screen.</p> <p>You can also set or change the user password from the phone screen menu <b>Applications</b>  &gt; <b>Device administration</b> &gt; <b>Set password</b>.</p> <p>A valid password must contain 4 to 127 characters from three out of the four types: capital letter, small letter, number, and special character.</p> <p>In the configuration file (cfg.xml), you can use the <b>User_Password</b> parameter to bypass the <b>Set password</b> screen that prompts on the first boot or after a factory reset. For more information, see <a href="#">Bypass the Set Password Screen, on page 104</a>.</p> <p>Default: Empty</p>
Phone-UI-User-Mode	<p>This parameter works only with the user access the (<b>ua</b>) attribute attached to an element tag in the configuration file (cfg.xml). You can restrict the parameters that the phone users see on the phone screen.</p> <p>When set to <b>Yes</b>, you can use the <b>ua</b> attribute to control user access to specific parameters on the phone screen menu. When set to <b>No</b>, the <b>ua</b> attribute isn't working.</p> <p>The options for the <b>ua</b> attribute are "na", "ro", and "rw". Parameters designated as "na" don't appear on the phone screen. Parameters designated as "ro" aren't editable by the user. Parameters designated as "rw" are editable by the user.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="672 1119 1321 1142">&lt;Phone-UI-User-Mode ua="na"&gt;No&lt;/Phone-UI-User-Mode&gt;</pre> </li> <li>In the phone web interface, set to <b>Yes</b> and then set the <b>ua</b> attribute of the desired parameter in the phone configuration file.</li> </ul> <p><b>Example:</b></p> <pre data-bbox="618 1293 1435 1392">&lt;Phone-UI-User-Mode ua="na"&gt;Yes&lt;/Phone-UI-User-Mode&gt; &lt;Enable_VLAN ua="ro"&gt;Yes&lt;/Enable_VLAN&gt; &lt;Preferred_Audio_Device ua="rw"&gt;Headset&lt;/Preferred_Audio_Device&gt; &lt;Block_ANC_Setting ua="na"&gt;Yes&lt;/Block_ANC_Setting&gt;</pre> <p>With the settings in the example, the user:</p> <ul style="list-style-type: none"> <li>Can see but can't change the setting of <b>VLAN</b> (<code>Enable_VLAN</code>) on the phone screen menu</li> <li>Can change the setting of <b>Preferred audio device</b> (<code>Preferred_Audio_Device</code>)</li> <li>Can't see the menu item <b>Block anonymous call</b> (<code>Block_ANC_Setting</code>) on the phone screen.</li> </ul> <p>Allowed values: Yes No</p> <p>Default: No</p>

Parameter Name	Description and Default Value
User Password Prompt	<p>Controls whether the user password setup screen prompts.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;User_Password_Prompt ua="na"&gt;Yes&lt;/User_Password_Prompt&gt;</pre> </li> <li>In the phone web interface, set to <b>Yes</b> to make the prompt available to the user.</li> </ul> <p>Allowed values: Yes No</p> <p>Default: Yes</p>

## Bypass the Set Password Screen



**Note** This feature isn't available from firmware release 11.2.3 and later.

You can bypass the phone **Set password** screen on the first boot or after a factory reset, based on these provisioning actions:

- DHCP configuration
- EDOS configuration
- User password configuration using in the phone XML configuration file

After the User Password is configured, the set password screen doesn't appear.

### Procedure

- 
- Step 1** Edit the phone `cfg.xml` file in a text or XML editor.
- Step 2** Insert the `<User_Password>` tag using one of these options.
- No password (start and end tag)—`<User_Password></User_Password>`
  - Password value (4-127 characters)—`<User_Password >Abc123</User_Password>`
  - No password (start tag only)—`<User_Password />`
- Step 3** Save the changes to the `cfg.xml` file.
- 

The **Set password** screen doesn't appear on the first boot or after a factory reset. If a password is specified, the user is prompted to enter the password when accessing the phone web interface or the phone screen menus.



## CHAPTER 8

# Third-Party Call Control Setup

---

- [Determine the Phone MAC Address, on page 105](#)
- [Network Configuration, on page 105](#)
- [Provisioning, on page 106](#)
- [Report Current Phone Configuration to the Provisioning Server, on page 106](#)

## Determine the Phone MAC Address

To add phones to the Third-Party Call Control system, determine the MAC address of a Cisco IP Phone.

### Procedure

---

Perform one of the following actions:

- On the phone, press **Applications** > **Status** > **Product Information**, and look at the MAC address field.
  - Look at the MAC label on the back of the phone.
  - Display the web page for the phone and select **Info** > **Status** > **Product Information**.
- 

## Network Configuration

The Cisco IP Phone is used as a part of a SIP network, because the phone supports Session Initiation Protocol (SIP). The Cisco IP Phone is compatible with other SIP IP PBX call control systems, such as BroadSoft, MetaSwitch, and Asterisk.

Configuration of these systems is not described in this document. For more information, see the documentation for the SIP PBX system to which you are connecting the Cisco IP Phone.

This document describes some common network configurations; however, your configuration can vary, depending on the type of equipment that your service provider uses.

## Provisioning

Phones can be provisioned to download configuration profiles or updated firmware from a remote server when they are connected to a network, when they are powered up, and at set intervals. Provisioning is typically part of high-volume, Voice-over-IP (VoIP) deployments and is limited to service providers. Configuration profiles or updated firmware are transferred to the device through use of TFTP, HTTP, or HTTPS.

## Report Current Phone Configuration to the Provisioning Server

You can configure the phone to report its full configuration, delta changes in the configuration, or the status data to the server. You can add up to two URLs in the **Report Rule** field to specify the destination for the report, and include an optional encryption key.

When requesting delta configuration and status reports at once, separate report rules with a **space**. Include a destination upload-URL in each of the report rules. You can optionally precede the report rule by one or more content arguments that are enclosed in square brackets [ ].

When a report upload is attempted, the **HTTP Report Method** field specifies whether the HTTP Request that the phone sends should be an **HTTP PUT** or an **HTTP POST**. Choose:

- **PUT Method**—To create a new report or overwrite an existing report at a known location on the server. For example, you may want to keep overwriting each report that you send and only store the most *current* configuration on the server.
- **POST Method**—To send the report data to the server for processing, such as, by a PHP script. This approach provides more flexibility for storing the configuration information. For example, you may want to send a series of phone status reports and store *all* the reports on the server.

Use the following content arguments in the **Report Rule** field to send specific configuration reports:

Content Argument	Report Content
Default: Blank	Full Configuration report
[ <b>--delta</b> ]	Configuration report contains <i>only</i> the latest changed fields  For example, <ul style="list-style-type: none"> <li>• Report 1 contains ABC changes.</li> <li>• Report 2 contains XYZ changes (<i>not</i> ABC and XYZ).</li> </ul>
[ <b>--status</b> ]	Full Phone Status report
<b>Note</b>	The preceding arguments can be combined with other arguments, such as, <b>--key</b> , <b>--uid</b> , and <b>--pwd</b> . These arguments control upload authentication and encryption, and are documented in the <b>Profile Rule</b> field.

- When you specify the [**--key <encryption key>**] argument in the **Report Rule**, the phone applies AES-256-CBC encryption to the file (configuration, status, or delta), with the specified encryption key.



**Note** If you have provisioned the phone with Input Keying Material (IKM) and want the phone to apply RFC 8188-based encryption to the file, do not specify the **--key** argument.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

- Step 1** Select **Voice > Provisioning > Upload Configuration Options**.
- Step 2** Set the parameter for each of the five fields as described in [Parameters for Reporting the Phone Configuration to the Server, on page 109](#).
- Step 3** Click **Submit All Changes**.

Example of user inputs and the resulting actions of the phone and provisioning server for the **Report Rule**:

- **HTTP PUT ALL configuration:**

If the HTTP report method is PUT, you enter the URL for the report rule in this format:

```
http://my_http_server/config-mpp.xml
```

Then the phone will report the configuration data to *http://my\_http\_server/config-mpp.xml*.

- **HTTP PUT Changed Configuration**

If the HTTP report method is PUT, you enter the URL for the report rule in this format:

```
[--delta]http://my_http_server/config-mpp-delta.xml;
```

Then the phone will report changed configuration to *http://my\_http\_server/config-mpp-delta.xml*.

- **HTTP PUT Encrypted Delta Configuration**

If the HTTP report method is PUT, you enter the URL for the report rule in this format:

```
[--delta --key test123]http://my_http_server/config-mpp-delta.enc.xml;
```

The phone will report status data to *http://my\_http\_server/config-mpp-delta.enc.xml*

On the report server side, the file can be decrypted like this: **# openssl enc -d -aes-256-cbc -k test123 -in config-mpp-delta.enc-delta.enc -out cfg.xml**

- **HTTP PUT Status Data**

If the HTTP report method is PUT, you enter the URL for the report rule in this format:

```
[--status]http://my_http_server/config-mpp-status.xml;
```

The phone will report status data to *http://my\_http\_server/config-mpp-status.xml*

- **HTTP PUT Changed Configuration and Status**

If the HTTP report method is PUT, you enter the URL for the report rule in this format:

```
[--status]http://my_http_server/config-mpp-status.xml
[--delta]http://my_http_server/config-mpp-delta.xml
```

The phone will report status data to *http://my\_http\_server/config-mpp-status.xml* and *http://my\_http\_server/config-mpp-delta.xml*

- **HTTP POST Changed Configuration**

If the report method is POST, you enter the URL for the report rule in this format:

```
[--delta]http://my_http_server/report_upload.php
```

The report upload file format"

```
// report_upload.php content
<?php
$filename = "report_cfg.xml"; // report file name
// where to put the file
$file = "/path/to/file".$filename;
// get data from http post
$report_data = file_get_contents('php://input');
// save the post data to file
$file_put_contents($file, $report_data);
?>
```

The phone will upload changed data to *http://my\_http\_server/report\_cfg.xml*

---

## Parameters for Reporting the Phone Configuration to the Server

Table 7: Parameters for Reporting the Phone Configuration to the Server

Field	Description
<b>Report Rule</b>	<p>Specifies how the phone reports its current internal configuration to the provisioning server. The URLs in this field specify the destination for a report and can include an encryption key.</p> <p>You can use the following keywords, encryption key, and file locations and names to control how you store the phone configuration information:</p> <ul style="list-style-type: none"> <li>• No keywords and <i>only</i> an XML file reports the <i>entire</i> configuration data to server.</li> <li>• <code>[--status]</code> keyword reports the <i>status data</i> to server.</li> <li>• <code>[--delta]</code> keyword reports the <i>changed</i> configuration to server.</li> <li>• <code>[--key &lt;encryption key&gt;]</code> keyword tells the phone to apply AES-256-CBC encryption with the specified encryption key to the configuration report, before sending it to the server.</li> </ul> <p>You can enclose the encryption key in double-quotes (") optionally.</p> <p><b>Note</b> If you have provisioned the phone with Input Keying Material (IKM) and want the phone to apply RFC 8188-based encryption to the file, do not specify a AES-256-CBC encryption key.</p> <ul style="list-style-type: none"> <li>• Two rules used together as:</li> </ul> <pre>[--delta]http://my_http_server/config-mpp-delta.xml [--status]http://my_http_server/config-mpp-status.xml</pre> <p><b>Caution</b> If you need to use the <code>[--delta]xml-delta</code> file rule and the <code>[--status]xml-status</code> file rule together, you must separate the two rules with a <b>space</b>.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>• In the phone configuration file with XML(cfg.xml), enter a string in this format:</li> </ul> <pre>&lt;Profile_Rule ua="na"&gt; [--delta]http://my_http_server/config-mpp-delta.xml [--status]http://my_http_server/config-mpp-status.xml &lt;/Profile_Rule&gt;</pre> <ul style="list-style-type: none"> <li>• In the phone web interface, enter the profile rule in this field.</li> </ul>

Field	Description
<b>HTTP Report method:</b>	<p>Specifies whether the HTTP Request that the phone sends should be an <i>PUT</i> or an <i>POST</i>.</p> <ul style="list-style-type: none"> <li>• <b>PUT</b>—To create a new report or overwrite an existing report at a known location on the server. For example, you may want to keep overwriting each report that you send and only store the most <i>current</i> configuration on the server.</li> <li>• <b>POST</b>—To send the report data to the server for processing, such as, by a PHP script. This approach provides more flexibility for storing the configuration information. For example, you may want to send a series of phone status reports and store <i>all</i> the reports on the server.</li> </ul> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>• In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;HTTP_Report_Method ua="na"&gt;PUT&lt;/HTTP_Report_Method&gt;</pre> </li> <li>• In the phone web interface, select an HTTP report method.</li> </ul> <p>Allowed values: PUT POST Default: POST</p>
<b>Report to Server:</b>	<p>Defines when the phone reports its configuration to the provisioning servers.</p> <ul style="list-style-type: none"> <li>• <b>On Request:</b> The phone reports its configuration only when an administrator sends a sip notify event, or the phone restarts.</li> <li>• <b>On Local Change:</b> The phone reports its configuration when any configuration parameter changes by an action on the phone or on the phone administration web page. The phone waits for a few seconds after a change is made, and then reports the configuration. This delay ensures that changes are reported to the web server in batches, rather than reporting a single change at a time.</li> <li>• <b>Periodically:</b> The phone reports its configuration at regular intervals. The interval is expressed in seconds.</li> </ul> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>• In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;Report_to_Server ua="na"&gt;Periodically&lt;/Report_to_Server&gt;</pre> </li> <li>• In the phone web interface, select an option from the list.</li> </ul> <p>Allowed values: On Request On Local Change Periodically Default: On Request</p>



Field	Description
<b>Periodic Upload to Server:</b>	<p>Defines the interval (in seconds) that the phone reports its configuration to the provisioning servers.</p> <p>This field is used only when <b>Report to Server</b> is set to <b>Periodically</b>.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;periodic_upload_to_server ua="na"&gt;3600&lt;/periodic_upload_to_server&gt;</pre> </li> <li>In the phone web interface, specify the interval in seconds.</li> </ul> <p>Allowed values: An integer ranging between 600 and 259200  Default: 3600</p>
<b>Upload Delay On Local Change:</b>	<p>Defines the delay (in seconds) that the phone waits after a change is made, and then reports the configuration.</p> <p>This field is used only when <b>Report to Server</b> is set to <b>On Local Change</b>.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;Upload_Delay_On_Local_Change ua="na"&gt;60&lt;/Upload_Delay_On_Local_Change&gt;</pre> </li> <li>In the phone web interface, specify the delay in seconds.</li> </ul> <p>Allowed values: An integer ranging between 10 and 900  Default: 60</p>





## CHAPTER 9

# Cisco IP Phone Security

---

- [Domain and Internet Setting](#), on page 113
- [Configure the Challenge for SIP INVITE Messages](#), on page 116
- [Transport Layer Security](#), on page 117
- [HTTPS Provisioning](#), on page 119
- [Enable the Firewall](#), on page 122
- [Configure Your Firewall with Additional Options](#), on page 123
- [Configure the Cipher List](#), on page 125
- [Enable Hostname Verification for SIP over TLS](#), on page 128
- [Enable Client-Initiated Mode for Media Plane Security Negotiations](#), on page 129
- [802.1X Authentication](#), on page 130
- [Set Up a Proxy Server](#), on page 132
- [Cisco Product Security Overview](#), on page 137

## Domain and Internet Setting

### Configure Restricted Access Domains

You can configure the phone to register, provision, firmware upgrade, and send reports using only the specified servers. Any registration, provisioning, upgrade, and report that don't use the specified servers can't be performed on the phone. If you specify the servers to use, ensure that the servers you enter in the following fields are included in the list:

- **Profile Rule**, **Profile Rule B**, **Profile Rule C**, and **Profile Rule D** on the **Provisioning** tab
- **Upgrade Rule** and **Cisco Headset Upgrade Rule** on the **Provisioning** tab
- **Report Rule** on the **Provisioning** tab
- **Custom CA Rule** on the **Provisioning** tab
- **Proxy** and **Outbound Proxy** on the **Ext (n)** tab

#### Before you begin

[Access the Phone Web Interface](#), on page 100.

### Procedure

---

- Step 1** Select **Voice > System**.
- Step 2** In the **System Configuration** section, locate the **Restricted Access Domains** field and enter fully qualified domain names (FQDNs) for each server. Separate FQDNs with commas.
- Example:**  
 voiceip.com, voiceipl.com
- You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:
- ```
<Restricted_Access_Domains ua="na">voiceip.com, voiceipl.com</Restricted_Access_Domains>
```
- Step 3** Click **Submit All Changes**.
- 

## Configure the DHCP Options

You can set the order in which your phone uses the DHCP options. For help with DHCP Options, see [DHCP Option Support, on page 115](#).

### Before you begin

[Access the Phone Web Interface, on page 100](#).

### Procedure

---

- Step 1** Select **Voice > Provisioning**.
- Step 2** In the **Configuration Profile** section, set the **DHCP Option To Use** and **DHCPv6 Option To Use** parameters as described in the [Parameters for DHCP Options Configuration, on page 114](#) table.
- Step 3** Click **Submit All Changes**.
- 

## Parameters for DHCP Options Configuration

The following table defines the function and usage of parameters for DHCP Options Configuration in the Configuration Profile section under the Voice>Provisioning tab in the phone web interface. It also defines

the syntax of the string that is added in the phone configuration file with XML(cfg.xml) code to configure a parameter.

**Table 8: Parameters for DHCP Options Configuration**

| Parameter            | Description   |
|----------------------|---|
| DHCP Option To Use   | <p>DHCP options, delimited by commas, used to retrieve firmware and profiles.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;DHCP_Option_To_Use ua="na"&gt;66,160,159,150,60,43,125&lt;/DHCP_Option_To_Use&gt;</pre> </li> <li>In the phone web page, enter the DHCP options separated by commas.</li> </ul> <p><b>Example:</b> 66,160,159,150,60,43,125</p> <p>Default: 66,160,159,150,60,43,125</p> |
| DHCPv6 Option To Use | <p>DHCPv6 options, delimited by commas, used to retrieve firmware and profiles.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;DHCPv6_Option_To_Use ua="na"&gt;17,160,159&lt;/DHCPv6_Option_To_Use&gt;</pre> </li> <li>In the phone web page, enter the DHCP options separated by commas.</li> </ul> <p><b>Example:</b> 17,160,159</p> <p>Default: 17,160,159</p>                                     |

## DHCP Option Support

The following table lists the DHCP options that are supported on the multiplatform phones.

| Network Standard | Description   |
|------------------|---|
| DHCP option 1    | Subnet mask   |
| DHCP option 2    | Time offset   |
| DHCP option 3    | Router  |
| DHCP option 6    | Domain name server  |
| DHCP option 15   | Domain name   |
| DHCP option 41   | IP address lease time   |
| DHCP option 42   | NTP server  |
| DHCP option 43   | <p>Vendor-specific information</p> <p>Can be used for TR.69 Auto Configurations Server (ACS) discovery.</p> |

| Network Standard | Description   |
|------------------|---|
| DHCP option 56   | NTP server<br>NTP server configuration with IPv6  |
| DHCP option 60   | Vendor class identifier   |
| DHCP option 66   | TFTP server name  |
| DHCP option 125  | Vendor-identifying vendor-specific information<br>Can be used for TR.69 Auto Configurations Server (ACS) discovery. |
| DHCP option 150  | TFTP server   |
| DHCP option 159  | Provisioning server IP  |
| DHCP option 160  | Provisioning URL  |

## Configure the Challenge for SIP INVITE Messages

You can set up the phone to challenge the SIP INVITE (initial) message in a session. The challenge restricts the SIP servers that are permitted to interact with devices on a service provider network. This practice prevents malicious attacks against the phone. When you enable this feature, authorization is required for initial incoming INVITE requests from the SIP proxy.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code.

### Before you begin

[Access the Phone Web Interface, on page 100.](#)

### Procedure

- 
- Step 1** Select **Voice > Ext(n)**, where n is an extension number.
- Step 2** In the **SIP Settings** section, select **Yes** from the **Auth INVITE** list to enable this feature or select **No** to disable it.
- You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:
- ```
<Auth_INVITE_1>Yes</Auth_INVITE_1_>
```
- Default: **No**.
- Step 3** Click **Submit All Changes**.
-

# Transport Layer Security

Transport Layer Security (TLS) is a standard protocol for securing and authenticating communications over the Internet. SIP over TLS encrypts the SIP signaling messages between the service provider SIP proxy and the end user.

The Cisco IP Phone uses UDP as the standard for SIP transport, but the phone also supports SIP over TLS for added security.

The following table describes the two TLS layers.

*Table 9: TLS Layers*

Protocol Name	Description
TLS Record Protocol	Layered on a reliable transport protocol, such as SIP or TCH, this layer ensures that the connection is private through use of symmetric data encryption and it ensures that the connection is reliable.
TLS Handshake Protocol	Authenticates the server and client, and negotiates the encryption algorithm and cryptographic keys before the application protocol transmits or receives data.

## Encrypt Signaling with SIP Over TLS

You can configure added security when you encrypt signaling messages with SIP over TLS.

### Before you begin

[Access the Phone Web Interface, on page 100](#). See [Transport Layer Security, on page 117](#)

### Procedure

**Step 1** Select **Voice > Ext(n)**, where n is an extension number.

**Step 2** In the **SIP Settings** section, select **TLS** from the **SIP Transport** list.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<SIP_Transport_1_ua="na">TLS</SIP_Transport_1_>
```

.

Options available:

- UDP
- TCP
- TLS
- Auto

Default: **UDP**.

**Step 3** Click **Submit All Changes**.

---

## Configure LDAP over TLS

You can configure LDAP over TLS (LDAPS) to enable secure data transmission between the server and a specific phone.



**Attention** Cisco recommends leaving the authentication method to the default value of **None**. Next to the server field is an authentication field that uses the values **None**, **Simple**, or **DIGEST-MD5**. There is no **TLS** value for authentication. The software determines the authentication method from the LDAPS protocol in the server string.

---

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

---

**Step 1** Select **Voice > Phone**.

**Step 2** In the **LDAP** section, enter a server address in the **Server** field.

You can also configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<LDAP_Server ua="na">ldaps://10.45.76.79</LDAP_Server>
```

For example, enter `ldaps://<ldaps_server>[:port]`.

where:

- **ldaps://** = The start of the server address string.
- **ldaps\_server** = IP address or domain name
- **port** = Port number. Default: 636

**Step 3** Click **Submit All Changes**.

---

## Configure StartTLS

You can enable Start Transport Layer Security (StartTLS) for the communications between the phone and the LDAP server. It uses the same network port (default 389) for both secure and insecure communications. If the LDAP server supports StartTLS, TLS encrypts the communications. Otherwise, the communications are in plaintext.



### Before you begin

- Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

---

**Step 1** Select **Voice > Phone**.

**Step 2** In the **LDAP** section, enter a server address in the **Server** field.

For example, enter `ldap://<ldap_server>[:port]`.

Where:

- **ldap://** = The start of the server address string, scheme of the URL
- **ldap\_server** = IP address or domain name
- **port** = Port number

You can also configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<LDAP_Server ua="na">ldap://<ldap_server>[:port]</LDAP_Server>
```

**Step 3** Set the **StartTLS Enable** field to **Yes**.

You can also configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<LDAP_StartTLS_Enable ua="na">Yes</LDAP_StartTLS_Enable>
```

**Step 4** Click **Submit All Changes**.

---

### Related Topics

[Parameters for LDAP Directory, on page 301](#)

## HTTPS Provisioning

The phone supports HTTPS for provisioning for increased security in managing remotely deployed units. Each phone carries a unique SLL Client Certificate (and associated private key), in addition to a Sipura CA server root certificate. The latter allows the phone to recognize authorized provisioning servers, and reject non-authorized servers. On the other hand, the client certificate allows the provisioning server to identify the individual device that issues the request.

For a service provider to manage deployment by using HTTPS, a server certificate must be generated for each provisioning server to which a phone resyncs by using HTTPS. The server certificate must be signed by the Cisco Server CA Root Key, whose certificate is carried by all deployed units. To obtain a signed server certificate, the service provider must forward a certificate signing request to Cisco, which signs and returns the server certificate for installation on the provisioning server.

The provisioning server certificate must contain the Common Name (CN) field, and the FQDN of the host running the server in the subject. It might optionally contain information following the host FQDN, separated by a slash (/) character. The following examples are of CN entries that are accepted as valid by the phone:

```
CN=sprov.callme.com
CN=pv.telco.net/mailto:admin@telco.net
CN=prof.voice.com/info@voice.com
```

In addition to verifying the server certificate, the phone tests the server IP address against a DNS lookup of the server name that is specified in the server certificate.

## Get a Signed Server Certificate

The OpenSSL utility can generate a certificate signing request. The following example shows the `openssl` command that produces a 1024-bit RSA public/private key pair and a certificate signing request:

```
openssl req -new -out provserver.csr
```

This command generates the server private key in `privkey.pem` and a corresponding certificate signing request in `provserver.csr`. The service provider keeps the `privkey.pem` secret and submits `provserver.csr` to Cisco for signing. Upon receiving the `provserver.csr` file, Cisco generates `provserver.crt`, the signed server certificate.

### Procedure

- 
- Step 1** Navigate to <https://software.cisco.com/software/cda/home> and log in with your CCO credentials.
- Note** When a phone connects to a network for the first time or after a factory reset, and there are no DHCP options set up, it contacts a device activation server for zero touch provisioning. New phones use “activate.cisco.com” instead of “webapps.cisco.com” for provisioning. Phones with firmware release earlier than 11.2(1) continue to use “webapps.cisco.com”. We recommend that you allow both the domain names through your firewall.
- Step 2** Select **Certificate Management**.
- On the **Sign CSR** tab, the CSR of the previous step is uploaded for signing.
- Step 3** From the **Select Product** drop-down list box, select **SPA1xx firmware 1.3.3 and newer/SPA232D firmware 1.3.3 and newer/SPA5xx firmware 7.5.6 and newer/CP-78xx-3PCC/CP-88xx-3PCC**.
- Step 4** In the **CSR File** field, click **Browse** and select the CSR for signing.
- Step 5** Select the encryption method:
- MD5
  - SHA1
  - SHA256
- Cisco recommends that you select SHA256 encryption.
- Step 6** From the **Sign in Duration** drop-down list box, select the applicable duration (for example, 1 year).
- Step 7** Click **Sign Certificate Request**.
- Step 8** Select one of the following options to receive the signed certificate:
- **Enter Recipient’s Email Address**—If you wish to receive the certificate via email, enter your email address in this field.

- **Download**—If you wish to download the signed certificate, select this option.

**Step 9** Click **Submit**.

The signed server certificate is either emailed to the email address previously provided or downloaded.

---

## Multiplatform Phone CA Client Root Certificate

Cisco also provides a Multiplatform Phone Client Root Certificate to the service provider. This root certificate certifies the authenticity of the client certificate that each phone carries. The Multiplatform Phones also support third-party signed certificates such as those provided by Verisign, Cybertrust, and so on.

To determine if a phone carries an individualized certificate, use the \$CCERT provisioning macro variable. The variable value expands to either Installed or Not Installed, according to the presence or absence of a unique client certificate. In the case of a generic certificate, it is possible to obtain the serial number of the unit from the HTTP request header in the User-Agent field.

HTTPS servers can be configured to request SSL certificates from connecting clients. If enabled, the server can use the Multiplatform Phone Client Root Certificate that Cisco supplies to verify the client certificate. The server can then provide the certificate information to a CGI for further processing.

The location for certificate storage may vary. For example, in an Apache installation, the file paths for storage of the provisioning server-signed certificate, its associated private key, and the Multiplatform Phone CA client root certificate are as follows:

```
# Server Certificate:
SSLCertificateFile /etc/httpd/conf/provserver.crt

# Server Private Key:
SSLCertificateKeyFile /etc/httpd/conf/provserver.key

# Certificate Authority (CA):
SSLCACertificateFile /etc/httpd/conf/spacroot.crt
```

For specific information, refer to the documentation for an HTTPS server.

The Cisco Client Certificate Root Authority signs each unique certificate. The corresponding root certificate is made available to service providers for client authentication purposes.

## Redundant Provisioning Servers

The provisioning server can be specified as an IP address or as a Fully Qualified Domain Name (FQDN). The use of an FQDN facilitates the deployment of redundant provisioning servers. When the provisioning server is identified through an FQDN, the phone attempts to resolve the FQDN to an IP address through DNS. Only DNS A-records are supported for provisioning; DNS SRV address resolution is not available for provisioning. The phone continues to process A-records until a server responds. If no server that is associated with the A-records responds, the phone logs an error to the syslog server.

## Syslog Server

If a syslog server is configured on the phone through use of the <Syslog Server> parameters, the resync and upgrade operations send messages to the syslog server. A message can be generated at the start of a remote file request (configuration profile or firmware load), and at the conclusion of the operation (indicating either success or failure).

The logged messages are configured in the following parameters and macro expanded into the actual syslog messages:

## Enable the Firewall

We have improved phone security by hardening the operating system. Hardening ensures that the phone has a firewall to protect it from malicious incoming traffic. The firewall tracks the ports for incoming and outgoing data. It detects incoming traffic from unexpected sources and blocks the access. Your firewall allows all outgoing traffic.

The firewall may dynamically unblock normally blocked ports. The outgoing TCP connection or UDP flow unblocks the port for return and continued traffic. The port is kept unblocked while flow is alive. The port reverts to blocked state when flow terminates or ages out.

The legacy setting, IPv6 Multicast Ping **Voice > System > IPv6 Settings > Broadcast Echo** continues to work independently of the new firewall settings.

Firewall configuration changes generally don't result in a phone restart. Phone soft restarts generally don't affect firewall operation.

The firewall is enabled by default. If it is disabled, you can enable it from the phone web page.

### Before you begin

[Access the Phone Web Interface, on page 100](#)

### Procedure

---

**Step 1** Select **Voice > System > Security Settings**.

**Step 2** In the **Firewall** drop down list, select **Enabled**.

You can also configure this parameter in the configuration file (cfg.xml) by entering a string in this format:

```
<Firewall ua="na">Enabled</Firewall>
```

The allowed values are Disabled|Enabled. The default value is Enabled.

**Step 3** Click **Submit All Changes**.

This enables the firewall with its default open UDP and TCP ports.

**Step 4** Select **Disabled** to disable the firewall if you wish your network to return to its prior behavior.

The following table describes the default open UDP ports.

Table 10: Firewall Default Open UDP Ports

Default Open UDP Port	Description
DHCP/DHCPv6	DHCP client Port 68 DHCPv6 client Port 546
SIP/UDP	Configure the Port in <b>Voice &gt; Ext&lt;n&gt; &gt; SIP Settings &gt; SIP Port</b> (example: 5060), when <b>Line Enable</b> is set to <b>Yes</b> , and <b>SIP Transport</b> is set to <b>UDP</b> or <b>Auto</b> .
RTP/RTCP	UDP port range from <b>RTP Port Min</b> to <b>RTP Port Max+1</b>
PFS (Peer Firmware Sharing)	Port 4051, when <b>Upgrade Enable</b> and <b>Peer Firmware Sharing</b> are set to <b>Yes</b> .
TFTP clients	Ports 53240-53245. You need this port range if the remote server uses a port other than the standard TFTP port 69. You may turn it off if the server uses standard port 69. See <a href="#">Configure Your Firewall with Additional Options, on page 123</a> .
TR-069	UDP/STUN port 7999, when <b>Enable TR-069</b> is set to <b>Yes</b> .

The following table describes the default open TCP ports.

Table 11: Firewall Default Open TCP Ports

Default Open TCP Port	Description
Web server	Port configured via Web Server Port (default 80), when <b>Enable Web Server</b> is set to <b>Yes</b> .
PFS (Peer Firmware Sharing)	Ports 4051 and 6970, when both <b>Upgrade Enable</b> and <b>Peer Firmware Sharing</b> are set to <b>Yes</b> .
TR-069	HTTP/SOAP port in TR-069 Connection Request URL, when <b>Enable TR-069</b> is set to <b>Yes</b> .  The port is chosen randomly from the range 8000-9999.

## Configure Your Firewall with Additional Options

You can configure additional options in the **Firewall Options** field. Type the keyword for each option in the field, and separate the keywords by commas (.). Some keywords have values. Separate the values by colons (:).

### Before you begin

[Access the Phone Web Interface, on page 100](#)

## Procedure

- Step 1** Go to **Voice > System > Security Settings**.
- Step 2** Select **Enabled** for the **Firewall** field.
- Step 3** In the **Firewall Options** field, enter the keywords. The list of ports applies to both IPv4 and IPv6 protocols. When you enter the keywords,
- separate the keywords with commas (,).
  - separate keywords values with colons (:).

**Table 12: Firewall Optional Settings**

Firewall Options Keywords	Description
Field is empty.	The firewall runs with default open ports.
NO_ICMP_PING	<p>The firewall blocks incoming ICMP/ICMPv6 <b>Echo</b> requests (Ping). This option may break some types of traceroute requests to the phone. Windows <b>tracert</b> is one example.</p> <p>Example <b>Firewall Options</b> entry with a combination of options: NO_ICMP_PING,TCP:12000,UDP:8000:8010</p> <p>The firewall runs with default settings and the following additional options:</p> <ul style="list-style-type: none"> <li>• Drops incoming ICMP/ICMPv6 <b>Echo</b> (Ping) requests.</li> <li>• Opens TCP port 12000 (IPv4 and IPv6) for incoming connections.</li> <li>• Opens UDP port range 8000-8010 (IPv4 and IPv6) for incoming requests.</li> </ul>
NO_ICMP_UNREACHABLE	<p>The phone doesn't send ICMP/ICMPv6 <i>Destination Unreachable</i> for UDP ports.</p> <p><b>Note</b> The exception is to always send <i>Destination Unreachable</i> for ports in the RTP port range.</p> <p>This option may break some types of <b>traceroute</b> requests to the device. For example, Linux <b>traceroute</b> may break.</p>
NO_CISCO_TFTP	<ul style="list-style-type: none"> <li>• The phone doesn't open TFTP-client port-range (UDP 53240:53245).</li> <li>• Requests to non-standard (non 69) TFTP server ports fail.</li> <li>• Requests to standard TFTP server port 69 work.</li> </ul>
The following keywords and options apply when the phone runs custom apps that handle incoming requests.	

Firewall Options Keywords	Description
UDP:<xxx>	Opens UDP port <xxx>.
UDP:<xxx:yyy>	Opens UDP port-range, <xxx to yyy>, inclusive.  You can have up to 5 UDP port options (single ports and port ranges). For example, you can have 3 UDP:<xxx> and 2 UDP:<xxx:yyy>.
TCP:<xxx>	Opens TCP port <xxx>.
TCP:<xxx:yyy>	Opens TCP port-range <xxx to yyy>, inclusive.  You can have up to 5 TCP port options (single ports and port ranges). For example, you can have 4 TCP:<xxx> and one TCP:<xxx:yyy>.

You can also configure this parameter in the configuration file (cfg.xml) by entering a string in this format:

```
<Firewall_Config ua="na">NO_ICMP_PING</Firewall_Config>
```

**Step 4** Click **Submit All Changes**.

## Configure the Cipher List

You can specify the cipher suites that the phone TLS applications use. The specified cipher list applies to all the applications that use the TLS protocol. The TLS applications on your phone include:

- Customer CA Provisioning
- E911 Geolocation
- Firmware/Cisco Headset Upgrade
- LDAPS
- LDAP (StartTLS)
- Picture Download
- Logo Download
- Dictionary Download
- Provisioning
- Report Upload
- PRT Upload
- SIP over TLS
- TR-069
- WebSocket API
- XML Services

- XSI Services

You can also specify the cipher suites with the TR-069 parameter (Device.X\_CISCO\_SecuritySettings.TLSCipherList) or with the the configuration file (cfg.xml). Enter a string in the configuration file in this format:

```
<TLS_Cipher_List ua="na">RSA:!aNULL:!eNULL</TLS_Cipher_List>
```

### Before you begin

Access the phone administration web page, see [Access the Phone Web Interface, on page 100](#).

### Procedure

**Step 1** Select **Voice > System**.

**Step 2** In the **Security Settings** section, enter the cipher suite or the combination of cipher suites in the **TLS Cipher List** field.

#### Example:

```
RSA:!aNULL:!eNULL
```

supports those cipher suites using RSA authentication, but excludes those cipher suites offering no encryption and authentication.

**Note** A valid cipher list must follow the format defined at <https://www.openssl.org/docs/man1.1.1/man1/ciphers.html>. Your phone doesn't support all the cipher strings listed on the OpenSSL web page. For the supported strings, see [Supported Cipher Strings, on page 127](#).

If the value in the **TLS Cipher List** field is blank or invalid, the cipher suites used vary with applications. See the following list for the suites that the applications use when this field is with a blank or an invalid value.

- Web Server (HTTPS) applications use the following cipher suites:
  - **ECDHE-RSA-AES256-GCM-SHA384**
  - **ECDHE-RSA-AES128-GCM-SHA256**
  - **AES256-SHA**
  - **AES128-SHA**
  - **DES-CBC3-SHA**
- XMPP uses the cipher list **HIGH:MEDIUM:AES:@STRENGTH**.
- SIP, TR-069, and other applications using the curl library use the **DEFAULT** cipher string. The **DEFAULT** cipher string contains the following cipher suites that the phone support:

```
DEFAULT Cipher Suites (28 suites):
ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
ECDHE_RSA_WITH_AES_256_GCM_SHA384
DHE_RSA_WITH_AES_256_GCM_SHA384
ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
ECDHE_RSA_WITH_AES_128_GCM_SHA256
```



```

DHE_RSA_WITH_AES_128_GCM_SHA256
ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
ECDHE_RSA_WITH_AES_256_CBC_SHA384
DHE_RSA_WITH_AES_256_CBC_SHA256
ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
ECDHE_RSA_WITH_AES_128_CBC_SHA256
DHE_RSA_WITH_AES_128_CBC_SHA256
ECDHE_ECDSA_WITH_AES_256_CBC_SHA
ECDHE_RSA_WITH_AES_256_CBC_SHA
DHE_RSA_WITH_AES_256_CBC_SHA
ECDHE_ECDSA_WITH_AES_128_CBC_SHA
ECDHE_RSA_WITH_AES_128_CBC_SHA
DHE_RSA_WITH_AES_128_CBC_SHA
RSA_WITH_AES_256_GCM_SHA384
RSA_WITH_AES_128_GCM_SHA256
RSA_WITH_AES_256_CBC_SHA256
RSA_WITH_AES_128_CBC_SHA256
RSA_WITH_AES_256_CBC_SHA
RSA_WITH_AES_128_CBC_SHA
EMPTY_RENEGOTIATION_INFO_SCSV

```

**Step 3** Click **Submit All Changes**.

## Supported Cipher Strings

The supported cipher strings listed following is based on the OpenSSL 1.1.1d standards.

**Table 13: Supported Cipher Strings (OpenSSL 1.1.1d)**

Strings	Strings	Strings
DEFAULT	kECDHE, kEECDH	CAMELLIA128, CAMELLIA256, CAMELLIA
COMPLEMENTOFDEFAULT	ECDHE, EECDH	CHACHA20
ALL	ECDH	SEED
COMPLEMENTOFALL	AECDH	MD5
HIGH	aRSA	SHA1, SHA
MEDIUM	aDSS, DSS	SHA256, SHA384
eNULL, NULL	aECDSA, ECDSA	SUITEB128, SUITEB128ONLY, SUITEB192
aNULL	TLSv1.2, TLSv1, SSLv3	
kRSA, RSA	AES128, AES256, AES	
kDHE, kEDH, DH	AESGCM	
DHE, EDH	AESCCM, AESCCM8	
ADH	ARIA128, ARIA256, ARIA	

# Enable Hostname Verification for SIP over TLS

You can enable increased phone security on a phone line if you use TLS. The phone line can verify the hostname to determine if the connection is secure.

Over a TLS connection, the phone can verify the hostname to check the server identity. The phone can check both the Subject Alternative Name (SAN) and the Subject Common Name (CN). If the hostname on the valid certificate matches the hostname that is used to communicate with the server, the TLS connection establishes. Otherwise, the TLS connection fails.

The phone always verifies the hostname for the following applications:

- LDAPS
- LDAP (StartTLS)
- XMPP
- Image upgrade over HTTPS
- XSI over HTTPS
- File download over HTTPS
- TR-069

When a phone line transports SIP messages over TLS, you can configure the line to enable or bypass the hostname verification with the **TLS Name Validate** field on the **Ext(n)** tab.

## Before you begin

- Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).
- On the **Ext(n)** tab, set **SIP Transport** to **TLS**.

## Procedure

---

**Step 1** Go to **Voice > Ext(n)**.

**Step 2** In the **Proxy and Registration** section, set the **TLS Name Validate** field to **Yes** to enable the hostname verification, or **No** to bypass the hostname verification.

You can also configure this parameter in the configuration file (cfg.xml) by entering a string in this format:

```
<TLS_Name_Validate_1_ua="na">Yes</TLS_Name_Validate_1_>
```

The allowed values are Yes or No. The default setting is Yes.

**Step 3** Click **Submit All Changes**.

---

# Enable Client-Initiated Mode for Media Plane Security Negotiations

To protect media sessions, you can configure the phone to initiate media plane security negotiations with the server. The security mechanism follows the standards stated in RFC 3329 and its extension draft *Security Mechanism Names for Media* (See <https://tools.ietf.org/html/draft-dawes-sipcore-mediasec-parameter-08#ref-2>). The transport of negotiations between the phone and the server can use SIP protocol over UDP, TCP, and TLS. You can limit that media plane security negotiation is applied only when the signaling transport protocol is TLS.

You can also configure the parameters in the configuration file (cfg.xml). To configure each parameter, see the syntax of the string in [Parameters for Media Plane Security Negotiation, on page 129](#).

## Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

## Procedure

- 
- |               |                                                                                                                                                                                                        |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Select <b>Voice &gt; Ext (n)</b> .                                                                                                                                                                     |
| <b>Step 2</b> | In the <b>SIP Settings</b> section, set the <b>MediaSec Request</b> and <b>MediaSec Over TLS Only</b> field as defined in <a href="#">Parameters for Media Plane Security Negotiation, on page 129</a> |
| <b>Step 3</b> | Click <b>Submit All Changes</b> .                                                                                                                                                                      |
- 

## Parameters for Media Plane Security Negotiation

The following table defines the function and usage of the parameters for media plane security negotiation in the **SIP Settings** section under the **Voice> Ext (n)** tab in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file (cfg.xml) with XML code to configure a parameter.

Table 14: Parameters for Media Plane Security Negotiation

Parameter	Description
MediaSec Request	<p>Specifies whether the phone initiates media plane security negotiations with the server.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;MediaSec_Request_1_ ua="na"&gt;Yes&lt;/MediaSec_Request_1_&gt;</pre> </li> <li>In the phone web interface, set this field to <b>Yes</b> or <b>No</b> as needed.</li> </ul> <p>Allowed values: Yes No</p> <ul style="list-style-type: none"> <li><b>Yes</b>—Client-initiated Mode. The phone initiates media plane security negotiations.</li> <li><b>No</b>—Server-initiated Mode. The server initiates media plane security negotiations. The phone doesn't initiate negotiations, but can handle negotiation requests from the server to establish secure calls.</li> </ul> <p>Default: No</p>
MediaSec Over TLS Only	<p>Specifies the signaling transport protocol over which media plane security negotiation is applied.</p> <p>Before setting this field to <b>Yes</b>, ensure that the signaling transport protocol is TLS.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;MediaSec_Over_TLS_Only_1_ ua="na"&gt;No&lt;/MediaSec_Over_TLS_Only_1_&gt;</pre> </li> <li>In the phone web interface, set this field to <b>Yes</b> or <b>No</b> as needed.</li> </ul> <p>Allowed values: Yes No</p> <ul style="list-style-type: none"> <li><b>Yes</b>—The phone initiates or handles media plane security negotiations only when the signaling transport protocol is TLS.</li> <li><b>No</b>—The phone initiates and handles media plane security negotiations regardless of the signaling transport protocol.</li> </ul> <p>Default: No</p>

## 802.1X Authentication

Cisco IP Phones use Cisco Discovery Protocol (CDP) to identify the LAN switch and determine parameters such as VLAN allocation and inline power requirements. CDP does not identify locally attached workstations.

Cisco IP Phones provide an EAPOL pass-through mechanism. This mechanism allows a workstation attached to the Cisco IP Phone to pass EAPOL messages to the 802.1X authenticator at the LAN switch. The pass-through mechanism ensures that the IP phone does not act as the LAN switch to authenticate a data endpoint before accessing the network.

Cisco IP Phones also provide a proxy EAPOL Logoff mechanism. In the event that the locally attached PC disconnects from the IP phone, the LAN switch does not see the physical link fail, because the link between the LAN switch and the IP phone is maintained. To avoid compromising network integrity, the IP phone sends an EAPOL-Logoff message to the switch on behalf of the downstream PC, which triggers the LAN switch to clear the authentication entry for the downstream PC.

Support for 802.1X authentication requires several components:

- Cisco IP Phone: The phone initiates the request to access the network. Cisco IP Phones contain an 802.1X supplicant. This supplicant allows network administrators to control the connectivity of IP phones to the LAN switch ports. The current release of the phone 802.1X supplicant uses the EAP-FAST and EAP-TLS options for network authentication.
- Cisco Secure Access Control Server (ACS) (or other third-party authentication server): The authentication server and the phone must both be configured with a shared secret that authenticates the phone.
- A LAN switch supporting 802.1X: The switch acts as the authenticator and pass the messages between the phone and the authentication server. After the exchange completes, the switch grants or denies the phone access to the network.

You must perform the following actions to configure 802.1X.


- Configure the other components before you enable 802.1X Authentication on the phone.
- Configure PC Port: The 802.1X standard does not consider VLANs and thus recommends that only a single device should be authenticated to a specific switch port. However, some switches support multidomain authentication. The switch configuration determines whether you can connect a PC to the PC port of the phone.
  - Yes: If you are using a switch that supports multidomain authentication, you can enable the PC port and connect a PC to it. In this case, Cisco IP Phones support proxy EAPOL-Logoff to monitor the authentication exchanges between the switch and the attached PC.
  - No: If the switch does not support multiple 802.1X-compliant devices on the same port, you should disable the PC Port when 802.1X authentication is enabled. If you do not disable this port and subsequently attempt to attach a PC to it, the switch denies network access to both the phone and the PC.
- Configure Voice VLAN: Because the 802.1X standard does not account for VLANs, you should configure this setting based on the switch support.
  - Enabled: If you are using a switch that supports multidomain authentication, you can continue to use the voice VLAN.
  - Disabled: If the switch does not support multidomain authentication, disable the Voice VLAN and consider assigning the port to the native VLAN.

## Enable 802.1X Authentication

You can enable 802.1X authentication on the phone. When 802.1X authentication is enabled, the phone uses 802.1X authentication to request network access. When 802.1X authentication is turned off, the phone uses CDP to acquire VLAN and network access. You can also view the transaction status on the phone screen menu.

### Procedure

- 
- Step 1** Perform one of the following actions to enable 802.1X authentication:
- In the phone web interface, select **Voice > System** and set the **Enable 802.1X Authentication** field to **Yes**. Then, click **Submit All Changes**.
  - In the configuration file (cfg.xml), entering a string in this format:
 

```
<Enable_802.1X_Authentication ua="rw">Yes</Enable_802.1X_Authentication>
```
  - On the phone, press **Applications**  **> Network configuration > Ethernet configuration > 802.1X authentication**. Then, toggle the **Device authentication** field to **On** with the **Select** button and press **Submit**.
- Step 2** (Optional) Select **Transaction status** to view the following:
- **Transaction status:** Displays the state of 802.1x authentication. The state can be
    - *Authenticating:* Indicates that the authentication process is in progress.
    - *Authenticated:* Indicates that the phone is authenticated.
    - *Disabled:* Indicates that 802.1x authentication is disabled on the phone.
  - **Protocol:** Displays the EAP method that is used for 802.1x authentication. The protocol can be EAP-FAST or EAP-TLS.
- Step 3** Press **Back** to exit the menu.
- 

## Set Up a Proxy Server

You can configure the phone to use a proxy server to enhance security. A proxy server acts as a firewall between the phone and Internet. After successful configuration, the phone connects to Internet through the proxy server which protects the phone from cyber attack.

You can set up a proxy server by either using an automatic configuration script or manually configuring the host server (hostname or IP address) and port of the proxy server.

When configured, the HTTP proxy feature applies to all the applications that use the HTTP protocol. The applications include the following:

- GDS (Activation Code Onboarding)
- EDOS Device Activation

- Onboarding to Webex Cloud (via EDOS and GDS)
- Certificate Authentication
- Provisioning
- Firmware Upgrade
- Phone Status Report
- PRT Upload
- XSI Services
- Webex Services

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

---

- Step 1** Select **Voice > System**.
- Step 2** In the section **HTTP Proxy Settings**, configure the parameter **Proxy Mode** and others according to your requirement. Detailed procedures are provided in the following steps.
- Step 3** Do one of the following actions:
- **Proxy Mode** is **Auto**:
    - If **Use Auto Discovery (WPAD)** is **Yes**, no further action is required. The phone will automatically retrieve a Proxy Auto-Configuration (PAC) file by the Web Proxy Auto-Discovery (WPAD) protocol.
    - If **Use Auto Discovery (WPAD)** is **No**, enter a valid URL in **PAC URL**.
  - **Proxy Mode** is **Manual**:
    - If **Proxy Server Requires Authentication** is **No**, enter a proxy server in **Proxy Host** and a proxy port in **Proxy Port**.
    - If **Proxy Server Requires Authentication** is **Yes**, enter a proxy server in **Proxy Host** and a proxy port in **Proxy Port**. And enter a username in **Username** and a password in **Password**.
  - **Proxy Mode** is **Off**, the HTTP proxy feature is disabled on the phone.
- You can also configure the parameters in the phone configuration file (cfg.xml). To configure each parameter, see the syntax of the string in the [Parameters for HTTP Proxy Settings, on page 134](#).
- Step 4** Click **Submit All Changes**.
-

## Parameters for HTTP Proxy Settings

The following table defines the function and usage of the HTTP proxy parameters in the **HTTP Proxy Settings** section under the **Voice > System** tab in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file (cfg.xml) with XML code to configure a parameter.

**Table 15: Parameters for HTTP Proxy Settings**

Parameter	Description and Default Value
Proxy Mode	<p>Specifies the HTTP proxy mode that the phone uses, or disables the HTTP proxy feature.</p> <ul style="list-style-type: none"> <li>• Auto           <p>The phone automatically retrieves a Proxy Auto-Configuration (PAC) file to select a proxy server. In this mode, you can determine whether to use Web Proxy Auto-Discovery (WPAD) protocol to retrieve a PAC file or manually enter a valid URL of the PAC file.</p> <p>For details about the parameters, see <a href="#">Use Auto Discovery (WPAD)</a> and <a href="#">PAC URL</a>.</p> </li> <li>• Manual           <p>You must manually specify a server (hostname or IP address) and a port of a proxy server.</p> <p>For details about the parameters, see <a href="#">Proxy Host</a> and <a href="#">Proxy Port</a>.</p> </li> <li>• Off           <p>You disable the HTTP proxy feature on the phone.</p> </li> </ul> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>• In the phone configuration file with XML(cfg.xml), enter a string in this format:           <pre>&lt;Proxy_Mode ua="rw"&gt;Off&lt;/Proxy_Mode&gt;</pre> </li> <li>• On the phone web interface, select a proxy mode or disable the feature.</li> </ul> <p>Allowed values: Auto, Manual, and Off Default: Off</p>



Parameter	Description and Default Value
Use Auto Discovery (WPAD)	<p>Determines whether the phone uses the Web Proxy Auto-Discovery (WPAD) protocol to retrieve a PAC file.</p> <p>WPAD protocol uses DHCP or DNS, or both network protocols to locate a Proxy Auto-Configuration (PAC) file automatically. PAC file is used to select a proxy server for a given URL. This file can be hosted locally or on a network.</p> <ul style="list-style-type: none"> <li>The parameter configuration takes effect when <b>Proxy Mode</b> is set to <b>Auto</b>.</li> <li>If you set the parameter to <b>No</b>, you must specify a PAC URL.</li> </ul> <p>For details about the parameter, see <a href="#">PAC URL</a>.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;Use_Auto_Discovery_WPAD_ua="rw"&gt;Yes&lt;/Use_Auto_Discovery_WPAD_&gt;</pre> </li> <li>On the phone web interface, select Yes or No as needed.</li> </ul> <p>Allowed values: Yes and No  Default: Yes</p>
PAC URL	<p>URL of a PAC file.</p> <p>For example, <code>http://proxy.department.branch.example.com</code></p> <p>TFTP, HTTP, and HTTPS are supported.</p> <p>If you set the <b>Proxy Mode</b> to <b>Auto</b> and <b>Use Auto Discovery (WPAD)</b> to <b>No</b>, you must configure this parameter.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;PAC_URL ua="rw"&gt;http://proxy.department.branch.example.com/pac&lt;/PAC_URL&gt;</pre> </li> <li>On the phone web interface, enter a valid URL that locates to a PAC file.</li> </ul> <p>Default: Empty</p>

Parameter	Description and Default Value
Proxy Host	<p>IP address or hostname of the proxy host server for the phone to access. For example:  <code>proxy.example.com</code></p> <p>The scheme (<code>http://</code> or <code>https://</code>) is not required.</p> <p>If you set the <b>Proxy Mode</b> to <b>Manual</b>, you must configure this parameter.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(<code>cfg.xml</code>), enter a string in this format:  <code>&lt;Proxy_Host ua="rw"&gt;proxy.example.com&lt;/Proxy_Host&gt;</code></li> <li>On the phone web interface, enter an IP address or hostname of the proxy server.</li> </ul> <p>Default: Empty</p>
Proxy Port	<p>Port number of the proxy host server.</p> <p>If you set the <b>Proxy Mode</b> to <b>Manual</b>, you must configure this parameter.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(<code>cfg.xml</code>), enter a string in this format:  <code>&lt;Proxy_Port ua="rw"&gt;3128&lt;/Proxy_Port&gt;</code></li> <li>On the phone web interface, enter a server port.</li> </ul> <p>Default: 3128</p>
Proxy Server Requires Authentication	<p>Determines whether the user needs to provide the authentication credentials (username and password) that the proxy server requires. This parameter is configured according to the actual behaviour of the proxy server.</p> <p>If you set the parameter to <b>Yes</b>, you must configure <b>Username</b> and <b>Password</b>.</p> <p>For details about the parameters, see <a href="#">Username</a> and <a href="#">Password</a>.</p> <p>The parameter configuration takes effect when <b>Proxy Mode</b> is set to <b>Manual</b>.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(<code>cfg.xml</code>), enter a string in this format:  <code>&lt;Proxy_Server_Requires_Authentication ua="rw"&gt;No&lt;/Proxy_Server_Requires_Authentication&gt;</code></li> <li>On the phone web interface, set this field Yes or No as needed.</li> </ul> <p>Allowed values: Yes and No</p> <p>Default: No</p>

Parameter	Description and Default Value
Username	<p>Username for a credential user on the proxy server.</p> <p>If <b>Proxy Mode</b> is set to <b>Manual</b> and <b>Proxy Server Requires Authentication</b> is set to <b>Yes</b>, you must configure the parameter.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;Proxy_Username ua="rw"&gt;Example&lt;/Proxy_Username&gt;</pre> </li> <li>On the phone web interface, enter the username.</li> </ul> <p>Default: Empty</p>
Password	<p>Password of the specified username for the proxy authentication purpose.</p> <p>If <b>Proxy Mode</b> is set to <b>Manual</b> and <b>Proxy Server Requires Authentication</b> is set to <b>Yes</b>, you must configure the parameter.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;Proxy_Password ua="rw"&gt;Example&lt;/Proxy_Password&gt;</pre> </li> <li>On the phone web interface, enter a valid password for the proxy authentication of the user.</li> </ul> <p>Default: Empty</p>

## Cisco Product Security Overview

This product contains cryptographic features and is subject to U.S. and local country laws that govern import, export, transfer, and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute, or use encryption. Importers, exporters, distributors, and users are responsible for compliance with U.S. and local country laws. By using this product, you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

Further information regarding U.S. export regulations can be found at <https://www.bis.doc.gov/policiesandregulations/ear/index.htm>.





## CHAPTER 10

# Phone Features and Setup

---

- [Phone Features and Setup Overview](#), on page 140
- [Cisco IP Phone User Support](#), on page 140
- [Telephony Features](#), on page 141
- [Feature Buttons and Softkeys](#), on page 149
- [Assign a Speed Dial Number](#), on page 150
- [DTMF Wait and Pause Parameters](#), on page 150
- [Enable Conference Button with a Star Code](#), on page 152
- [Configure Alphanumeric Dialing](#), on page 153
- [Set the Optional Network Configuration](#), on page 154
- [XML Services](#), on page 158
- [Shared Lines](#), on page 164
- [Assign a Ringtone to an Extension](#), on page 168
- [Enable Hoteling on a Phone](#), on page 171
- [Enable Flexible Seating on a Phone](#), on page 172
- [Enable Extension Mobility on a Phone](#), on page 172
- [Set the User Password](#), on page 173
- [Download Problem Reporting Tool Logs](#), on page 174
- [Configure Problem Report Tool](#), on page 174
- [Server-Configured Paging](#), on page 178
- [Configure Multicast Paging](#), on page 178
- [Configure a Phone to Accept Pages Automatically](#), on page 182
- [Manage Phones with TR-069](#), on page 182
- [View TR-069 Status](#), on page 183
- [Set up a Secure Extension](#), on page 189
- [Configure the SIP Transport](#), on page 189
- [Block Non-Proxy SIP Messages to a Phone](#), on page 190
- [Configure a Privacy Header](#), on page 191
- [Enable P-Early-Media Support](#), on page 192
- [Enable Peer Firmware Sharing](#), on page 192
- [Specify the Profile Authentication Type](#), on page 194
- [Control the Authentication Requirement to Access the Phone Menus](#), on page 195
- [Silence an Incoming Call with Ignore Soft Key](#), on page 197
- [Move an Active Call from a Phone to Other Phones \(Locations\)](#), on page 197

- [Sync the Block Caller ID Feature with the Phone and the BroadWords XSI Server, on page 201](#)
- [Enable Viewing BroadWorks XSI Call Logs on a Line , on page 202](#)
- [Enable Feature Key Sync, on page 205](#)
- [DND and Call Forward Status Sync, on page 206](#)
- [Enable Synchronization of Anonymous Call Rejection via XSI Service, on page 208](#)
- [Enable Synchronization of Call Waiting via XSI Service, on page 210](#)
- [Enable End-of-Call Statistics Reports in SIP Messages, on page 212](#)
- [SIP Session ID, on page 214](#)
- [Set Up a Phone for Remote SDK, on page 216](#)
- [Hide a Menu Item from Being Displayed on the Phone Screen, on page 218](#)
- [Display Caller Number Instead of Unresolved Caller Name, on page 221](#)
- [Menu Shortcuts Mapping on PSK, on page 222](#)
- [Add a Menu Shortcut to a Programmable Softkey, on page 225](#)
- [Enable LDAP Unified Search, on page 226](#)

## Phone Features and Setup Overview

After you install Cisco IP Phones in your network, configure their network settings, and add them to Third-Party Call Control System, you must use the Third-Party Call Control System to configure telephony features, optionally modify phone templates, set up services, and assign users.

You can modify additional settings for the Cisco IP Phone from Third-Party Call Control Configuration Utility. Use this web-based application to set up phone registration criteria and calling search spaces, to configure corporate directories and services, and to modify phone button templates, among other tasks.

## Cisco IP Phone User Support

If you are a system administrator, you are likely the primary source of information for Cisco IP Phone users in your network or company. It is important to provide current and thorough information to end users.

To successfully use some of the features on the Cisco IP Phone (including Services and voice message system options), users must receive information from you or from your network team or must be able to contact you for assistance. Make sure to provide users with the names of people to contact for assistance and with instructions for contacting those people.

We recommend that you create a web page on your internal support site that provides end users with important information about their Cisco IP Phones.

Consider including the following types of information on this site:

- User guides for all Cisco IP Phone models that you support
- Information on how to access the Cisco Unified Communications Self Care Portal
- List of features supported
- User guide or quick reference for your voicemail system

# Telephony Features

After you add Cisco IP Phones to Third-Party Call Control system, you can add functionality to the phones. The following table includes a list of supported telephony features, many of which you can configure by using Third-Party Call Control system.



**Note** The Third-Party Call Control system also provides several service parameters that you can use to configure various telephony functions.

Feature	Description and More Information
AES 256 Encryption Support for Phones	Enhances security by supporting TLS 1.2 and new ciphers.
Alphanumeric Dialing	Allows users to place a call with alphanumeric characters. You can use these characters for alphanumeric dialing: a-z, A-Z, 0-9, -, _, ., and +.
Any Call Pickup	Allows users to pick up a call on any line in their call pickup group, regardless of how the call was routed to the phone.
Assisted Directed Call Park	Enables users to park a call by pressing only one button using the Direct Park feature. Administrators must configure a Busy Lamp Field (BLF) Assisted Directed Call Park button. When users press an idle BLF Assisted Directed Call Park button for an active call, the active call is parked at the Direct Park slot associated with the Assisted Directed Call Park button.
Audio Settings	Configures audio settings for the phone speaker, the handset, and the headsets that are connected to the phone.
Auto Answer	Connects incoming calls automatically after a ring or two. Auto Answer works with either the speakerphone or the headset.
Blind Transfer	Blind Transfer: This transfer joins two established calls (call is in hold or in connected state) into one call and drops the feature initiator from the call. Blind Transfer does not initiate a consultation call and does not put the active call on hold.  Some JTAPI/TAPI applications are not compatible with the Join and Blind Transfer feature implementation on the Cisco IP Phone and you may need to configure the Join and Direct Transfer Policy to disable join and direct transfer on the same line or possibly across lines.
Busy Lamp Field (BLF)	Allows user to monitor call state of a directory number.
Busy Lamp Field (BLF) Pickup	Allows user to pick up incoming calls to the directory number monitored through BLF.
Call Back	Provides users with an audio and visual alert on the phone when a busy or unavailable party becomes available.
Call Display Restrictions	Determines the information that will display for calling or connected lines, depending on the parties who are involved in the call. RPID and PAID caller id handling are supported.

Feature	Description and More Information
Call Forward	Allows users to redirect incoming calls to another number. Call Forward services include Call Forward All, Call Forward Busy, Call Forward No Answer.
Call Forward Destination Override	Allows you to override Call Forward All (CFA) in cases where the CFA target places a call to the CFA initiator. This feature allows the CFA target to reach the CFA initiator for important calls. The override works whether the CFA target phone number is internal or external.
Call Forward Notification	Allows you to configure the information that the user sees when receiving a forwarded call.
Call History for Shared Line	Allows you to view shared line activity in the phone Call History. This feature: <ul style="list-style-type: none"> <li>• Logs missed calls for a shared line.</li> <li>• Logs all answered and placed calls for a shared line.</li> </ul>
Call Park	Allows users to park (temporarily store) a call and then retrieve the call by using another phone.
Call Pickup	Allows users to redirect a call that is ringing on another phone within their pickup group to their phone.  You can configure an audio and visual alert for the primary line on the phone. This alert notifies the users that a call is ringing in their pickup group.
Call Waiting	Indicates (and allows users to answer) an incoming call that rings while on another call. Incoming call information appears on the phone display.
Caller ID	Caller identification such as a phone number, name, or other descriptive text appear on the phone display.
Caller ID Blocking	Allows a user to block their phone number or name from phones that have caller identification enabled.
Calling Party Normalization	Calling party normalization presents phone calls to the user with a dialable phone number. Any escape codes are added to the number so that the user can easily connect to the caller again. The dialable number is saved in the call history and can be saved in the Personal Address Book.
Cisco Extension Mobility	Allows users to temporarily access their Cisco IP Phone configuration such as line appearances, services, and speed dials from shared Cisco IP Phone by logging into the Cisco Extension Mobility service on that phone when they log into the Cisco Extension Mobility service on that phone.  Cisco Extension Mobility can be useful if users work from a variety of locations within your company or if they share a workspace with coworkers.
Cisco Extension Mobility Cross Cluster (EMCC)	Enables a user configured in one cluster to log into a Cisco IP Phone in another cluster. Users from a home cluster log into a Cisco IP Phone at a visiting cluster.  <b>Note</b> Configure Cisco Extension Mobility on Cisco IP Phones before you configure EMCC.



Feature	Description and More Information
Cisco WebDialer	Allows users to make calls from web and desktop applications.
Classic Ringtone	Supports narrowband and wideband ringtones. The feature makes the available ringtones common with other Cisco IP Phones.
Client Matter Code (CMC)	Enables a user to specify that a call relates to a specific client matter.
Conference	<p>Allows a user to talk simultaneously with multiple parties by calling each participant individually.</p> <p>Allows a noninitiator in a standard (ad hoc) conference to add or remove participants; also allows any conference participant to join together two standard conferences on the same line.</p> <p><b>Note</b> Be sure to inform your users whether these features are activated.</p>
Configurable RTP/sRTP Port Range	<p>Provides a configurable port range (Port Min to Port Max) for Real-Time Transport Protocol (RTP) and secure Real-Time Transport Protocol (sRTP).</p> <p>The value range for the Port Min and Port Max is 2048 to 49151.</p> <p>The default RTP and sRTP port range is 16384 to 16482.</p> <p><b>Note</b> If the value range (Port Max - Port Min) is less than 16 or you use an incorrect port range, the port range (16382 to 32766) is used instead.</p> <p>You configure the RTP and sRTP port range in the SIP Profile.</p>
Contacts Management of the BroadSoft Personal Directory on the Phone	<p>Provides the user with the ability to add, edit, and delete in the BroadSoft Personal directory. Allows the user to add contacts from recent calls or any types of directories (if enabled).</p> <p>In addition administrator can set the BroadSoft Personal directory as the target directory to store new contacts.</p>
CTI Applications	A computer telephony integration (CTI) route point can designate a virtual device to receive multiple, simultaneous calls for application-controlled redirection.
Device Invoked Recording	<p>Provides end users with the ability to record their telephone calls via a softkey.</p> <p>In addition administrators may continue to record telephone calls via the CTI User Interface.</p>
Directed Call Park	<p>Allows a user to transfer an active call to an available directed call park number that the user dials or speed dials. A Call Park BLF button indicates whether a directed call park number is occupied and provides speed-dial access to the directed call park number.</p> <p><b>Note</b> If you implement Directed Call Park, avoid configuring the Park softkey. This prevents users from confusing the two Call Park features.</p>
Directed Call Pickup	Allows a user to pick up a ringing call on a DN directly by pressing the GPickUp softkey and entering the directory number of the device that is ringing.
Divert	Allows a user to transfer a ringing, connected, or held call directly to a voice-messaging system. When a call is diverted, the line becomes available to make or receive new calls.

Feature	Description and More Information
Do Not Disturb (DND)	When DND is turned on, either no audible rings occur during the ringing-in state of a call, or no audible or visual notifications of any type occur.
DND and Call Forward Indication on Non-selected Line Key	Displays the DND and call forward icons next the to the line key label. The line key should be enabled with feature key sync. The line key should also be enabled with DND or call forward.
Emergency Calls	Enables users to make emergency calls. The emergency services receive the phone's location and a call-back number, to use when the emergency call unexpectedly disconnects.
EnergyWise	Enables an IP Phone to sleep (power down) and wake (power up) at predetermined times, to promote energy savings.
Enhanced Secure Extension Mobility Cross Cluster (EMCC)	Improves the Secure Extension Mobility Cross Cluster (EMCC) feature by preserving the network and security configurations on the login phone. By so doing, security policies are maintained, network bandwidth is preserved and network failure is avoided within the visiting cluster (VC).
Extension Mobility Size Safe and Feature Safe	With Feature Safe, your phone can use any phone button template that has the same number of line buttons that the phone model supports.  Size Safe allows your phone to use any phone button template that is configured on the system.
Forced Authorization Code (FAC)	Controls the types of calls that certain users can place.
Feature Activation Code	Allows a user to enable, disable, or configure the Call Forward All service.
Headset Sidetone Control	Allows an administrator to set the sidetone level of a wired headset.
Group Call Pickup	Allows a user to answer a call that is ringing on a directory number in another group.
Hold Status	Enables phones with a shared line to distinguish between the local and remote lines that placed a call on hold.
Hold/Resume	Allows the user to move a connected call from an active state to a held state. <ul style="list-style-type: none"> <li>• No configurations are required unless you want to use Music On Hold. See “Music On Hold” in this table.</li> <li>• See “Hold Reversion” in this table.</li> </ul>
HTTP Download	Enhances the file download process to the phone to use HTTP by default. If the HTTP download fails, the phone reverts to using the TFTP download.
HTTP Proxy	Allows you to set up a proxy server for the phone.
HTTPS for Phone Services	Increases security by requiring communication using HTTPS.  <b>Note</b> When the web is in HTTPS mode, the phone is an HTTPS server.
Improve Caller Name and Number Display	Improves the display of caller names and numbers. If the Caller Name is known, then the Caller Number is displayed instead of Unknown.

Feature	Description and More Information
IPv6 Support	Provides support for expanded IP addressing on Cisco IP Phones. IPv6 support is provided in standalone or in dual-stack configurations. In dual-stack mode, the phone is able to communicate using IPv4 and IPv6 simultaneously, independent of the content.
Jitter Buffer	The Jitter Buffer feature handles jitter from 10 milliseconds (ms) to 1000 ms for both audio and video streams.
Join Across Lines	Allows users to combine calls that are on multiple phone lines to create a conference call.  Some JTAPI/TAPI applications are not compatible with the Join and Direct Transfer feature implementation on the Cisco IP Phone and you may need to configure the Join and Direct Transfer Policy to disable join and direct transfer on the same line or possibly across lines.
Join	Allows users to combine two calls that are on one line to create a conference call and remain on the call.
Line Display Enhancement	Improves Call Display by removing the central dividing line when it is not required. This feature applies to the Cisco IP Phone 7841 only.
Log out of hunt groups	Allows users to log out of a hunt group and temporarily block calls from ringing their phone when they are not available to take calls. Logging out of hunt groups does not prevent nonhunt group calls from ringing their phone.
Malicious Caller Identification (MCID)	Allows users to notify the system administrator about suspicious calls that are received.
Meet Me Conference	Allows a user to host a Meet Me conference in which other participants call a predetermined number at a scheduled time.
Message Waiting	Defines directory numbers for message waiting on and off indicators. A directly-connected voice-message system uses the specified directory number to set or to clear a message waiting indication for a particular Cisco IP Phone.
Message Waiting Indicator	When you have a message, a message displays on the phone screen. Your phone also provides an audible message waiting indicator.
Minimum Ring Volume	Sets a minimum ringer volume level for an IP phone.
Missed Call Logging	Allows a user to specify whether missed calls will be logged in the missed calls directory for a given line appearance.
Mobile Connect	Enables users to manage business calls using a single phone number and pick up in-progress calls on the desk phone and a remote device such as a mobile phone. Users can restrict the group of callers according to phone number and time of day.
Mobile Voice Access	Extends Mobile Connect capabilities by allowing users to access an interactive voice response (IVR) system to originate a call from a remote device such as a cellular phone.

Feature	Description and More Information
Monitoring and Recording	<p>Allows a supervisor to silently monitor an active call. The supervisor cannot be heard by either party on the call. The user might hear a monitoring audible alert tone during a call when it is being monitored.</p> <p>When a call is secured, the security status of the call is displayed as a lock icon on Cisco IP Phones. The connected parties might also hear an audible alert tone that indicates the call is secured and is being monitored.</p> <p><b>Note</b> When an active call is being monitored or recorded, the use can receive or place intercom calls; however, if the user place an intercom call, the active call will be put on hold, which causes the recording session to terminate and the monitoring session to suspend. To resume the monitoring session, the party whose call is being monitored must resume the call.</p>
Multicasting Paging	Enables users to page some or all phones. If the phone is on an active call while a group page starts, the incoming page is ignored.
Multiple Calls Per Line Appearance	<p>Each line can support multiple calls. By default, the phone supports two active calls per line, and a maximum of ten active calls per line. Only one call can be connected at any time; other calls are automatically placed on hold.</p> <p>The system allows you to configure maximum calls/busy trigger not more than 10/6. Any configuration more than 10/6 is not officially supported.</p>
Music On Hold	Plays music while callers are on hold.
Mute	Mutes the handset or headset microphone.
No Alert Name	Makes it easier for end users to identify transferred calls by displaying the original caller's phone number. The call appears as an Alert Call followed by the caller's telephone number.
Onhook Dialing	Allows a user to dial a number without going off hook. The user can then either pick up the handset or press Dial.
Other Group Pickup	Allows a user to answer a call ringing on a phone in another group that is associated with the user's group.
Pause in Speed Dial	Users can set up the speed-dial feature to reach destinations that require Forced Authorization Code (FAC) or Client Matter Code (CMC), dialing pauses, and additional digits (such as a user extension, a meeting access code, or a voicemail PIN) without manual intervention. When the user presses the speed dial, the phone establishes the call to the specified DN and sends the specified FAC, CMC, and DTMF digits to the destination and inserts the necessary dialing pauses.

Feature	Description and More Information
Peer Firmware Sharing (PFS)	<p>Allows IP Phones located at remote sites to share the firmware files amongst them, which saves bandwidth when the upgrade process takes place. This feature uses Cisco Peer-to-Peer-Distribution Protocol (CPPDP) which is a Cisco proprietary protocol used to form a peer-to-peer hierarchy of devices. CPPDP is also used to copy firmware or other files from peer devices to the neighbouring devices.</p> <p>PFS aids in firmware upgrades in branch/remote office deployment scenarios that run over bandwidth-limited WAN links.</p> <p>Provides the following advantages over the traditional upgrade method:</p> <ul style="list-style-type: none"> <li>• Limits congestion on TFTP transfers to centralized remote TFTP servers</li> <li>• Eliminates the need to manually control firmware upgrades</li> <li>• Reduces phone downtime during upgrades when large numbers of devices are reset simultaneously</li> </ul> <p>The more the number of IP phones, the better it's performance compared to the traditional firmware upgrade method.</p>
PLK Support for Queue Statistics	<p>The PLK Support for Queue Statistics feature enables the users to query the call queue statistics for hunt pilots and the information appears on phone screen.</p>
Plus Dialing	<p>Allows the user to dial E.164 numbers prefixed with a plus (+) sign.</p> <p>To dial the + sign, the user needs to press and hold the star (*) key for at least 1 second. This applies to dialing the first digit for an on-hook (including edit mode) or off-hook call.</p>
Power Negotiation over LLDP	<p>Allows the phone to negotiate power using Link Level Endpoint Discovery Protocol (LLDP) and Cisco Discovery Protocol (CDP).</p>
Problem Reporting Tool	<p>Submits phone logs or reports problems to an administrator.</p>
Programmable Feature Buttons	<p>You can assign features, such as New Call, Call Back, and Call Forward All to line buttons.</p>
Quality Reporting Tool (QRT)	<p>Allows users to submit information about problem phone calls by pressing a button. QRT can be configured for either of two user modes, depending upon the amount of user interaction desired with QRT.</p>
Redial	<p>Allows users to call the most recently dialed phone number by pressing a button or the Redial softkey.</p>
Remote Customization (RC)	<p>Allows a service provider to customize the phone remotely. There is no need for either the service provider to physically touch the phone or a user to configure the phone. The service provider can work with a sales engineer at the time of ordering to set this up.</p>
Ringtone Setting	<p>Identifies ring type used for a line when a phone has another active call.</p>
Reverse Name Lookup	<p>Identifies the caller name using the incoming or outgoing call number. You must configure either the LDAP Directory or the XML directory. You can enable or disable the reverse name lookup using the phone administration web page.</p>

Feature	Description and More Information
RTCP Hold For SIP	Ensures that held calls are not dropped by the gateway. The gateway checks the status of the RTCP port to determine if a call is active or not. By keeping the phone port open, the gateway will not end held calls.
Secure Conference	<p>Allows secure phones to place conference calls using a secured conference bridge. As new participants are added by using Confrn, Join, cBarge softkeys or MeetMe conferencing, the secure call icon displays as long as all participants use secure phones.</p> <p>The Conference List displays the security level of each conference participant. Initiators can remove nonsecure participants from the Conference List. Noninitiators can add or remove conference participants if the Advanced Adhoc Conference Enabled parameter is set.</p>
Serviceability for SIP Endpoints	<p>Enables administrators to quickly and easily gather debug information from phones.</p> <p>This feature uses SSH to remotely access each IP phone. SSH must be enabled on each phone for this feature to function.</p>
Shared Line	Allows a user with multiple phones to share the same phone number or allows a user to share a phone number with a coworker.
Show Caller Name and Caller Number	<p>The phones can display both the caller name and caller number for incoming calls. The phone screen size limits the length of the caller name and the caller number that display.</p> <p>If boxes are displayed in the caller name, follow the procedure in <a href="#">Display Caller Number Instead of Unresolved Caller Name, on page 221</a>.</p> <p>This feature applies to the incoming call alert only and doesn't change the Call Forward and Hunt Group features.</p> <p>See "Caller ID" in this table.</p>
Show Product Configuration Version	Allows you to customize the product configuration version that shows on the phone screen <b>Product information</b> .
Show Duration for Call History	<p>Displays the time duration of placed and received calls in the Call History details.</p> <p>If the duration is greater than or equal to one hour, the time is displayed in the Hour, Minute, Second (HH:MM:SS) format.</p> <p>If the duration is less than one hour, the time is displayed in the Minute, Second (MM:SS) format.</p> <p>If the duration is less than one minute, the time is displayed in the Second (SS) format.</p>
Silence Incoming Call	Allows you to silence an incoming call by pressing <b>Ignore</b> softkey or by pressing the volume button down.
Speed Dial	Dials a specified number that has been previously stored.
Synchronization of Call Waiting and Anonymous Call Rejection	Allows you to enable or disable synchronization of the Call Waiting and Anonymous Call Rejection functions between a specific line and a BroadSoft XSI server.
Time Zone Update	Updates the Cisco IP Phone with time zone changes.

Feature	Description and More Information
Transfer	Allows users to redirect connected calls from their phones to another number.  Some JTAPI/TAPI applications are not compatible with the Join and Direct Transfer feature implementation on the Cisco IP Phone and you may need to configure the Join and Direct Transfer Policy to disable join and direct transfer on the same line or possibly across lines.
Voice Message System	Enables callers to leave messages if calls are unanswered.
Web Access Enable by Default	Web services are enabled by default.
XSI call logs display	Allows you to configure a phone to display recent call logs from either the BroadWorks server or the local phone. After you enable the feature, the <b>Recents</b> screen has a <b>Display recents from</b> menu and the user can choose the XSI call logs or the local call logs.

## Feature Buttons and Softkeys

The following table provides information about features that are available on softkeys, features that are available on dedicated feature buttons, and features that you need to configure as programmable feature buttons. A “Supported” entry in the table indicates that the feature is supported for the corresponding button type or softkey. Of the two button types and softkeys, only programmable feature buttons require configuration in the web interface or in the configuration file (cfg.xml).



**Note** The Cisco IP Conference Phone 8832 Multiplatform Phones doesn't have programmable feature buttons.

**Table 16: Features with Corresponding Buttons and Softkeys**

Feature Name	Dedicated Feature Button	Softkey
Answer	Not supported	Supported
Call Forward All	Not supported	Supported
Call Forward Busy	Not supported	Supported
Call Forward No Answer	Not supported	Supported
Call Park	Not supported	Supported
Call Pickup (Pick Up)	Not supported	Supported
Category	Not supported	Supported
Conference	Not supported	Supported (only displayed during connected call conference scenario)
Divert	Not supported	Supported

Feature Name	Dedicated Feature Button	Softkey
Do Not Disturb	Not supported	Supported
Hold	Not supported	Supported
Mute	Supported	Not supported
Redial	Not supported	Supported
Speed Dial	Not supported	Supported
Transfer	Not supported	Supported (only displayed during connected call transfer scenario)

## Assign a Speed Dial Number

You can configure speed dials on the phone with the web interface. The user can see the configured speed dials on the phone and can use the speed dial number to call the corresponding contact.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

**Step 1** Select **Voice > User**.

**Step 2** In the **Speed Dial** section, enter a name in **Speed Dial (n) Name** and the number in **Speed Dial (n) Number** that corresponds to the speed dial entry.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code. The speed dial parameters are line-specific. Enter a string in the format

```
<Speed_Dial_1_Name ua="rw">John Wood</Speed_Dial_1_Name>
<Speed_Dial_1_Number ua="rw">12345678</Speed_Dial_1_Number>
```

**Step 3** Click **Submit All Changes**.

## DTMF Wait and Pause Parameters

Speed dial, directory, extended function, and other strings configured in the phone can include *wait* (X) and *pause* (,) characters. These characters that allow manual and automatic DTMF (Dual-Tone Multi-Frequency) signal transmission.

You can add the wait and pause character with speed-dial, extended function, or directory strings in the format:

```
{Dial_String}[ ][,|X][DTMF_string][,|X][DTMF_string]
```

where:



- `Dial_String`—is the number that the user is trying to reach. For example, 8537777 or 14088537777.
- `[ ]`(space)—is a dial termination character that defines or delimits the end of the dial string. The space is mandatory. If the phone encounters an X or a comma (,) before the space, the characters are treated as part of dial string.
- `,` (comma)—is a 2-second pause that is inserted for each comma in the string.
- `X` (wait)—indicates that the phone is waits for user input and acknowledgement.

When the user manually enters the DTMF signal with the key pad, the user sees a message to acknowledge that the transmission of the manual entry is complete. On confirmation, the phone sends any DTMF signals defined by the *DTMF\_string*. The phone executes the next parameter. If there are no more parameters in the dial string to execute, the phone exits to the main screen.

The wait prompt window does not disappear until the user confirms the wait prompt or the call is ended either by the user or ended by the remote device.

- `DTMF_string`—is the DTMF signals that a user sends to a remote device after the call is connected. The phone cannot send signals other than valid DTMF signals.

#### Example:

```
18887225555,,5552X2222
```

A speed dial entry triggers the phone to dial 18887225555. The space indicates the end of the dial string. The phone waits 4 seconds (2 commas), and then sends the DTMF signals 5552.

A message is displayed, prompting the user to manually enter digits. When the user finishes dialing the digits, the user presses **OK** to confirm the manual input is complete. The phone sends the DTMF signals 2222.

#### Usage Guidelines

A user can transmit digits any time, as long as the call is connected.

The maximum length of the string, including the Xs or commas (,), is limited to the length of a speed-dial entry, dial screen entry, directory entry, and other dialed strings.

When a wait is initiated, the phone displays the home screen and prompts the user to input more digits with the key pad. If this action occurs while the user is editing an entry, the edits might be lost.

If only the first part of a dial string matches a dial plan when the call is dialed, the portion of the dial string that does not match the dial string is ignored. For example:

```
85377776666, , 1, 23
```

If 8537777 matches a dial plan, the characters 6666 are ignored. The phone waits 4 seconds before sending DTMF 1. It then wait 2 seconds and sends DTMF 23.

When logging the call, the phone only logs the dial string; the DTMF strings are not logged.

Valid DTMF signals are 0-9, \*, or #. All other characters are ignored.

#### Limitations

When the call is connected and immediately transferred, the phone might not be able to process the DTMF signals. This depends on the length of time that the call is connected before it is transferred.

# Enable Conference Button with a Star Code

You can add a star code to the Conference button so that your user can press the button only once to add many active calls to a conference. You can enable this feature from the phone web page.

## Before you begin

- The phone server must support this feature.
- Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

## Procedure

---

**Step 1** Select **Voice > Ext(n)**, where n is an extension number.

**Step 2** In the **Call Features Settings** section, configure the **Conference Single Hardkey** and **Conference Bridge URL** fields as defined in [Conference Button Parameters, on page 152](#).

You can also enable the conference button with a xml file. Enter a string in this format:

```
<Conference_Bridge_URL_1_ ua="na">*55</Conference_Bridge_URL_1_>
<Conference_Single_Hardkey_1_ ua="na">Yes</Conference_Single_Hardkey_1_>
```

**Step 3** Click **Submit All Changes**.

---

## Conference Button Parameters

The following table defines the function and usage of the conference button parameters in the **Call Features Settings** section under the **Voice > Ext (n)** tab in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file (cfg.xml) with XML code to configure a parameter.

Table 17: Conference Button Parameters

Parameter	Description and default value
Conference Single Hardkey	<p>You can use this field to specify whether to use only the Conferenc button on the key to initiate a conference call. When set to <b>Yes</b>, the user can use only the Conference button to initiate a conference call. The <b>Conf</b> softkey is deactivated. When set to <b>No</b>, the user can use both the Conference button and the <b>Conf</b> softkey.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;Conference_Single_Hardkey_1_ua="na"&gt;Yes&lt;/Conference_Single_Hardkey_1_&gt;</pre> </li> <li>In the phone web interface, set this field to <b>Yes</b> or <b>No</b> to enable or disable this feature.</li> </ul> <p>Allowed values: Yes No</p> <p>Default: No</p>
Conference Bridge URL	<p>URL used to join a conference call, generally in the form of a dialable number or a URI in this format <code>user@IPaddress:port</code>.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;Conference_Bridge_URL_1_ua="na"&gt;*55&lt;/Conference_Bridge_URL_1_&gt;</pre> </li> <li>in the phone web interface, specify the URI or a number as the conference bridge.</li> </ul> <p>Default: Empty</p>

## Configure Alphanumeric Dialing

You can configure a phone so that the user of the phone can make a call by dialing alphanumeric characters instead of dialing only digits. In the phone web page, you can configure alphanumeric dialing with speed-dial, blf, and call pickup.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

**Step 1** Select **Voice > Ext (n)**.

**Step 2** In the **Dial Plan** section, set **Enable URI Dialing** to **Yes** to enable alphanumeric dialing.

You can also configure the parameter in the configuration file (cfg.xml). The parameter is line-specific.

```
<Enable_URI_Dialing_1_ua="na">Yes</Enable_URI_Dialing_1_>
```

**Step 3** Select **Voice > Phone**, you can add a string on a line key in this format to enable speed dial with alphanumeric dialing capability:

```
fnc=sd;ext=xxxx.yyyy@$PROXY;nme=yyyy,xxxx
```

For example:

```
fnc=sd;ext=first.last@$PROXY;nme=Last,First
```

The above example will enable the user to dial "first.last" to make a call.

**Note** The supported characters that you can use for alphanumeric dialing are a-z, A-Z, 0-9, -, \_, ., and +.

**Step 4** Click **Submit All Changes**.

---

## Set the Optional Network Configuration

Optional network servers provide resources such as DNS lookup, network time, logging, and device discovery. It also enables you to add PC port mirroring on the user phone. Your user can also enable or disable this service from the phone.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code. To configure each parameter, see the syntax of the string in [Parameters for Optional Network Configuration, on page 154](#).

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

---

**Step 1** Select **Voice > System**.

**Step 2** In the **Optional Network Configuration** section, set up the fields as described in [Parameters for Optional Network Configuration, on page 154](#).

**Step 3** Click **Submit All Changes**.

---

## Parameters for Optional Network Configuration

The following table defines the function and usage of the access control parameters in the **Optional Network Configuration** section under the **Voice > System** tab in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file (cfg.xml) with XML code to configure a parameter.

Table 18: Parameters for Optional Network Configuration

Parameter	Description and Default Value
Host Name	<p>The hostname of the server that the phone uses.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;Host_Name ua="rw"&gt;serverhost.com&lt;/Host_Name&gt;</pre> </li> <li>On the phone web interface, enter the host name of the server to use.</li> </ul> <p>Default: Empty</p>
Domain	<p>The network domain of the Phone.</p> <p>If you're using LDAP, see <a href="#">LDAP Configuration, on page 301</a>.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;Domain ua="rw"&gt;domainexample.com&lt;/Domain&gt;</pre> </li> <li>In the phone web interface, enter the domain of the phone.</li> </ul> <p>Default: Empty</p>
DNS Server Order	<p>Specifies the sequence for selecting the DNS server.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>Manual, DHCP</li> <li>Manual</li> <li>DHCP, Manual</li> </ul> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;DNS_Server_Order ua="na"&gt;Manual,DHCP&lt;/DNS_Server_Order&gt;</pre> </li> <li>In the phone web interface, specify the order that the phone follows to select the DNS server.</li> </ul> <p>Allowed values: Manual,DHCP Manual DHCP,Manual</p> <p>Default: Manual, DHCP</p>
DNS Query Mode	<p>Specifies the mode of DNS query.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;DNS_Query_Mode ua="na"&gt;Parallel&lt;/DNS_Query_Mode&gt;</pre> </li> <li>In the phone web interface, select the mode of DNS query.</li> </ul> <p>Allowed values: Parallel Sequential</p> <p>Default: Parallel</p>

Parameter	Description and Default Value
DNS Caching Enable	<p>Enables or disables DNS caching. When enabled, the DNS query results are cached. The phone retrieves the local DNS cache until the local cache is expired. When disabled, the phone always performs DNS queries.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>• In the phone configuration file with XML(cfg.xml), enter a string in this format:  <code>&lt;DNS_Caching_Enable ua="na"&gt;Yes&lt;/DNS_Caching_Enable&gt;</code></li> <li>• In the phone web interface, set this field to <b>Yes</b> or <b>No</b> to enable or disable DNS caching.</li> </ul> <p>Allowed values: Yes No  Default: Yes</p>
Switch Port Config	<p>Allows you to select speed and duplex of the network port. Values are:</p> <ul style="list-style-type: none"> <li>• Auto</li> <li>• 10 HALF</li> <li>• 10 FULL</li> <li>• 100 HALF</li> <li>• 100 FULL</li> </ul> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>• In the phone configuration file with XML(cfg.xml), enter a string in this format:  <code>&lt;Switch_Port_Config ua="na"&gt;AUTO&lt;/Switch_Port_Config&gt;</code></li> <li>• On the phone web interface, select the speed for the port or select <b>Auto</b> to allow the system to select the speed.</li> </ul> <p>Default: Auto</p>

Parameter	Description and Default Value
PC Port Config	<p>Allows you to select Speed and duplex of the Computer (access) port.</p> <ul style="list-style-type: none"> <li>• Auto</li> <li>• 10 HALF</li> <li>• 10 FULL</li> <li>• 100 HALF</li> <li>• 100 FULL</li> </ul> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>• In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;PC_Port_Config ua="na"&gt;AUTO&lt;/PC_Port_Config&gt;</pre> </li> <li>• In the phone web interface, select the speed for the port or select <b>Auto</b> to allow the system to select the speed.</li> </ul> <p>Default: Auto</p>
PC PORT Enable	<p>Enables or disables the PC port on the phone.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>• In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;PC_PORT_Enable ua="na"&gt;Yes&lt;/PC_PORT_Enable&gt;</pre> </li> <li>• In the phone web interface, set this field to <b>Yes</b> or <b>No</b> to enable or disable the PC port on the phone.</li> </ul> <p>Allowed values: Yes No</p> <p>Default: Yes</p>
Enable PC Port Mirror	<p>Enables or disables PC Port mirroring on the phone. When set to <b>Yes</b>, you can see the packets on the phone.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>• In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;Enable_PC_Port_Mirror ua="na"&gt;No&lt;/Enable_PC_Port_Mirror&gt;</pre> </li> <li>• In the phone web interface, set this field to <b>Yes</b> or <b>No</b> to enable or disable PC port mirroring on the phone.</li> </ul> <p>Allowed values: Yes No</p> <p>Default: No</p>
Syslog Server	See <a href="#">System Log Parameters, on page 36</a> .
Syslog identifier	See <a href="#">System Log Parameters, on page 36</a> .

Parameter	Description and Default Value
Primary NTP Server	<p>IP address or name of the primary NTP server used to synchronize its time.</p> <p>You can set primary NTP server for both IPv4 and IPv6.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;Primary_NTP_Server ua="rw"&gt;192.168.1.10&lt;/Primary_NTP_Server&gt;</pre> </li> <li>In the phone web interface, specify the IP address or host name of the NTP server.</li> </ul> <p>Default: Blank</p>
Secondary NTP Server	<p>IP address or name of the secondary NTP server used to synchronize its time.</p> <p>You can set primary NTP server for both IPv4 and IPv6.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;Secondary_NTP_Server ua="rw"&gt;192.168.1.11&lt;/Secondary_NTP_Server&gt;</pre> </li> <li>In the phone web interface, specify the IP address or host name of the NTP server.</li> </ul> <p>Default: Blank</p>
Use Config TOS	<p>This field controls whether the phone uses the Time of Service (TOS) parameters on the <b>Ext (n)</b> tab. Set this field to <b>Yes</b> when you want the phones to use the TOS configuration specified on the <b>Ext (n)</b> tab. Otherwise, set this field to <b>No</b>.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;Use_Config_TOS ua="na"&gt;No&lt;/Use_Config_TOS&gt;</pre> </li> <li>In the phone web interface, select Yes or No as needed.</li> </ul> <p>Allowed values: Yes No</p> <p>Default: No</p>

## XML Services

The phones provide support for XML services, such as an XML Directory Service or other XML applications. For XML services, only HTTP and HTTPS support is available.

The following Cisco XML objects are supported:

- CiscoIPPhoneMenu
- CiscoIPPhoneText
- CiscoIPPhoneInput
- CiscoIPPhoneDirectory



- CiscoIPPhoneIconMenu
- CiscoIPPhoneStatus
- CiscoIPPhoneExecute
- CiscoIPPhoneImage
- CiscoIPPhoneImageFile
- CiscoIPPhoneGraphicMenu
- CiscoIPPhoneFileMenu
- CiscoIPPhoneStatusFile
- CiscoIPPhoneResponse
- CiscoIPPhoneError
- CiscoIPPhoneGraphicFileMenu
- Init:CallHistory
- Key:Headset
- EditDial:n

The full list of supported URIs is contained in *Cisco Unified IP Phone Services Application Development Notes for Cisco Unified Communications Manager and Multiplatform Phones*, located here:

## XML Directory Service

When an XML URL requires authentication, use the parameters **XML UserName** and **XML Password**.

The parameter **XML UserName** in XML URL is replaced by \$XML UserName.

For example:

The parameter XML UserName is **cisco**. The XML Directory Service URL is **http://www.sipurash.com/path?username=\$XML\_User\_Name**.

This results in the request URL: **http://www.sipurash.com/path?username=cisco**.

## Configure a Phone to Connect to an XML Application

You can also configure the parameters in the configuration file (cfg.xml) as defined in [Parameters for XML Applications, on page 160](#).

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

- 
- Step 1** Select **Voice > Phone**.

- Step 2** In the **XML Service** section, configure the **XML Application Service Name** and **XML Application Service URL** fields as defined in [Parameters for XML Applications, on page 160](#).
- Step 3** (Optional) Specify the username and password to authenticate XML service in the **XML User Name** and **XML Password** fields as defined in [Parameters for XML Applications, on page 160](#).
- Step 4** (Optional) Enable and configure authentication for CGI/Execute URL via Post from an external application (for example, a web application) to the phones.
- Configure the **CISCO XML EXE Enable** and **CISCO XML EXE Auth Mode** fields as defined in [Parameters for XML Applications, on page 160](#).
- Step 5** Click **Submit All Changes**.

## Parameters for XML Applications

The following table defines the function and usage of the XML application parameters in the **XML Service** section under the **Voice > Phone** tab in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file (cfg.xml) with XML code to configure a parameter.

*Table 19: Parameters for XML Applications*

Parameter	Description
XML Application Service Name	<p>Name of the XML application. The name displays on the phone as a web application choice.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;XML_Application_Service_Name ua="na"&gt;XML_APP&lt;/XML_Application_Service_Name&gt;</pre> </li> <li>In the phone web interface, enter a name for the XML application.</li> </ul> <p>Default: Empty</p>
XML Application Service URL	<p>The URL where the XML application is located.</p> <p>Macro variables are supported in XML URLs. For the valid macro variables, see <a href="#">Macro Variables, on page 162</a>.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;XML_Application_Service_URL ua="na"&gt;XML_APP&lt;/XML_Application_Service_URL&gt;</pre> </li> <li>In the phone web interface, enter the URL for the XML application.</li> </ul> <p>Default: Empty</p>

Parameter	Description
XML User Name	<p>XML service username for authentication purposes.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;XML_User_Name ua="na"&gt;username&lt;/XML_User_Name&gt;</pre> </li> <li>In the phone web interface, enter the username used for authenticating XML service.</li> </ul> <p>Default: Empty</p>
XML Password	<p>XML service password for the specified XML User Name. The password you entered in this field shows in the configuration file (cfg.xml) as</p> <pre>&lt;!-- &lt;XML_Password ua="na"&gt;*****&lt;/XML_Password&gt; --&gt;</pre> <p>Default: Empty</p>
CISCO XML EXE Enable	<p>Specifies whether authentication is required to access the XML application server.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;CISCO_XML_EXE_Enable ua="na"&gt;Yes&lt;/CISCO_XML_EXE_Enable&gt;</pre> </li> <li>In the phone web interface, set it to <b>Yes</b> or <b>No</b> to enable or disable authentication.</li> </ul> <p>Allowed values: No</p> <p>Default: No</p>
CISCO XML EXE Auth Mode	<p>Specifies the authentication mode for Cisco XML EXE. The available options are:</p> <ul style="list-style-type: none"> <li>Trusted—No authentication is performed regardless of the local credential.</li> <li>Local Credential—Authentication is based on the digest authentication using the local credential, if set. If the local credential is not set, then no authentication is performed.</li> <li>Remote Credential—Authentication is based on the digest authentication using the remote credential as set in the XML application on the web page (to access an XML application server).</li> </ul> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;CISCO_XML_EXE_Auth_Mode ua="na"&gt;Local Credential&lt;/CISCO_XML_EXE_Auth_Mode&gt;</pre> </li> <li>In the phone web interface, select an authentication mode.</li> </ul> <p>Allowed values: Trusted Local Credential Remote Credential</p> <p>Default: Local Credential</p>

## Macro Variables

You can use macro variables in XML URLs. The following macro variables are supported:

- User ID—UID1, UID2 to UIDn
- Display name—DISPLAYNAME1, DISPLAYNAME2 to DISPLAYNAMEn
- Auth ID—AUTHID1, AUTHID2 to AUTHIDn
- Proxy—PROXY1, PROXY2 to PROXYn
- MAC Address using lowercase hex digits—MA
- Product Name—PN
- Product Series Number—PSN
- Serial Number—SERIAL\_NUMBER

The following table shows the list of macros supported on the phones:

Macro Name	Macro Expansion
\$	The form \$\$ expands to a single \$ character.
A through P	Replaced by general-purpose parameters GPP_A through GPP_P.
SA through SD	Replaced by special purpose parameters GPP_SA through GPP_SD. These parameters hold keys or passwords used in provisioning.  <b>Note</b> \$SA through \$SD are recognized as arguments to the optional resync URL qualifier, --key.
MA	MAC address using lowercase hex digits (000e08aabbcc).
MAU	MAC address using uppercase hex digits (000E08AABBCC).
MAC	MAC address using lowercase hex digits with a colon to separate hex digit pairs (00:0e:08:aa:bb:cc).
PN	
PSN	
SN	Serial Number string; for example, 88012BA01234.
CCERT	SSL Client Certificate status, installed or not installed.
IP	IP address of the phone within its local subnet; for example, 192.168.1.100.
EXTIP	External IP of the phone, as seen on the internet; for example, 66.43.16.52.

Macro Name	Macro Expansion
SWVER	<p>Software version string. Use the software version string to compare against the current phone's firmware load.</p> <p>Follow the format below:</p> <ul style="list-style-type: none"> <li>For Firmware Release 11.3(1)SR1 and previous:  <code>sipyyyy.11-0-1MPP-376</code>            where <i>yyyy</i> indicates the phone model or phone series; <i>11</i> is the major version; <i>0</i> is the minor version; <i>1MPP</i> is the micro version; and <i>376</i> is the build number.</li> <li>For Firmware Release 11.3(2) and later:  <code>sipyyyy.11-3-2MPP0001-609</code>            where <i>yyyy</i> indicates the phone model or phone series; <i>11</i> is the major version; <i>3</i> is the minor version; <i>2MPP0001</i> is the micro version; and <i>609</i> is the build number.</li> </ul> <p>There are two methods to compare firmware loads:</p> <ul style="list-style-type: none"> <li><b>With quotes, "\$SWVER"</b>—Variable acts as a string in firmware load name comparisons. For "<code>\$SWVER</code>" eq "<code>sipyyyy.11-2-1MPP-312.loads</code>" or "<code>\$SWVER</code>" eq "<code>sipyyyy.11-3-2MPP0001-609.loads</code>", the phone model number and the version numbers in the load name are part of the comparison.</li> <li><b>Without quotes, \$SWVER</b>—Variable is parsed to determine a build number, plus major, minor, and micro revision numbers. For example, when the <code>sip88xx.11-3-2MPP0001-598.loads</code> and <code>sip8845_65.11-3-2MPP0001-598.loads</code> firmware names are parsed, the result ignores the model number and load number. The result for both firmware names yields a major revision=11, minor revision=3, micro revision=2MPP0001, and build number=598.</li> </ul> <p>See more information about firmware version comparison, see <a href="#">Macro Expansion Variables, on page 69</a>.</p>
HWVER	Hardware version string; for example, 1.88.1.
PRVST	<p>Provisioning State (a numeric string):</p> <ul style="list-style-type: none"> <li>-1 = explicit resync request</li> <li>0 = power-up resync</li> <li>1 = periodic resync</li> <li>2 = resync failed, retry attempted</li> </ul>
UPGST	<p>Upgrade State (a numeric string):</p> <ul style="list-style-type: none"> <li>1 = first upgrade attempt</li> <li>2 = upgrade failed, retry attempt</li> </ul>
UPGERR	Result message (ERR) of previous upgrade attempt; for example, http_get failed.


Macro Name	Macro Expansion
PRVTMR	Seconds since last resync attempt.
UPGTMR	Seconds since last upgrade attempt.
REGTMR1	Seconds since Line 1 lost registration with SIP server.
REGTMR2	Seconds since Line 2 lost registration with SIP server.
UPGCOND	Legacy macro name.
SCHEME	File access scheme (TFTP, HTTP, or HTTPS, obtained after parsing resync or upgrade URL).
METH	Deprecated alias for SCHEME, do not use.
SERV	Request target server hostname.
SERVIP	Request target server IP address (following DNS lookup).
PORT	Request target UDP/TCP port.
PATH	Request target file path.
ERR	Result message of resync or upgrade attempt.
UIDn	The contents of the Line n UserID configuration parameter.
ISCUST	If unit is customized, value=1, otherwise 0. <b>Note</b> Customization status viewable on Web UI Info page.
INCOMINGNAME	Name associated with first connected, ringing, or inbound call.
RE MOTENUMBER	Phone number of first connected, ringing, or inbound call. If there are multiple calls, the data associated with the first call found is provided.
DISPLAYNAMEn	The contents of the Line N Display Name configuration parameter.
AUTHIDn	The contents of the Line N auth ID configuration parameter.

## Shared Lines

A shared line is a directory number that appears on more than one phone. You can create a shared line by assigning the same directory number to various phones.

Incoming calls display on all phones that share a line, and anyone can answer the call. Only one call remains active at a time on a phone.

Call information displays on all phones that are sharing a line. If somebody turns on the privacy feature, you do not see the outbound calls made from the phone. However, you see inbound calls to the shared line.

All phones with a shared line ring when a call is made to the line. If you place the shared call on hold, anyone shared with the line can resume the call by pressing  or the **Resume** softkey.

The following shared line features are supported:

- Line Seizure
- Public Hold
- Private Hold
- Silent Barge (only through enabled programmable softkey)

The following features are supported as for a private line

- Transfer
- Conference
- Call Park / Call Retrieve
- Call Pickup
- Do Not Disturb
- Call Forward

You can configure each phone independently. Account information is usually the same for all IP phones, but settings such as the dial plan or preferred codec information can vary.

## Configure a Shared Line

You can create a shared line by assigning the same directory number to more than one phone on the phone web page.

You can also configure the parameters in the phone configuration file with XML (cfg.xml) code. To configure each parameter, see the syntax of the string in [Parameters for Configuring a Shared Line, on page 166](#).

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

- 
- Step 1** Select **Voice > Ext(n)**, where **(n)** is the number of an extension to share.
  - Step 2** In the **General** section, set the **Line Enable** parameter as described in the [Parameters for Configuring a Shared Line, on page 166](#) table.
  - Step 3** In the **Share Line Appearance** section, set **Share Ext**, **Shared User ID field**, **Subscription Expires**, and **Restrict MWI** parameters as described in the [Parameters for Configuring a Shared Line, on page 166](#) table.
  - Step 4** In the **Proxy and Registration** section, enter the IP address of the proxy server in the **Proxy** field.

You can also configure this parameter in the configuration file (cfg.xml) by entering a string in this format:

```
<Proxy_1_ ua="na">aslbsoft.sipurash.com</Proxy_1_>
```

Example for proxy server address: aslbsoft.sipurash.com

**Step 5** In the **Subscriber Information** section, enter the **Display Name** and **User ID** (extension number) for the shared extension.

You can also configure this parameter in the configuration file (cfg.xml) by entering a string in this format:

```
<Display_Name_1_ ua="na">name</Display_Name_1_>
<User_ID_1_ ua="na">4085273251</User_ID_1_>
```

**Step 6** In the **Miscellaneous Line Key Settings** section, set **SCA Barge-In Enable** parameter as described in the [Parameters for Configuring a Shared Line, on page 166](#) table.

**Step 7** Click **Submit All Changes**.

## Parameters for Configuring a Shared Line

The following table describes the parameters in the **Voice > Ext(n)** tab of the phone web page.

The following table defines the function and usage of Shared Line parameters in the General and Share Line Appearance sections under the Ext(n) tab in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file with XML(cfg.xml) code to configure a parameter.

**Table 20: Parameters for Shared Lines**

Parameter	Description
Line Enable	<p>Enables a line for the service.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone web interface, select <b>yes</b> to enable. Otherwise, select <b>No</b>.</li> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;Line_Enable_1_ ua="na"&gt;Yes&lt;/Line_Enable_1_&gt;</pre> </li> </ul> <p>Valid values: Yes No</p> <p>Default: Yes</p>
Share Ext	<p>Indicates whether other Cisco IP phones share this extension is, or the extension is private.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone web interface, select <b>yes</b> to enable. Otherwise, select <b>No</b>.</li> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;Share_Ext_1_ ua="na"&gt;No&lt;/Share_Ext_1_&gt;</pre> </li> </ul> <p>If you set <b>Share Ext</b> to <b>No</b>, this extension is private and doesn't share calls, regardless of the <b>Share Line Appearance</b> setting. If you set this extension to <b>Yes</b>, calls follow the <b>Share Line Appearance</b> setting.</p> <p>Valid values: Yes No</p> <p>Default: Yes</p>



Parameter	Description
Shared User ID	<p>The user identified assigned to the shared line appearance.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone web interface, enter the user ID.</li> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;Shared_User_ID_1_ ua="na"&gt;Shared UserID&lt;/Shared_User_ID_1_&gt;</pre> </li> </ul>
Subscription Expires	<p>Number of seconds before the SIP subscription expires. Before the subscription expiration, the phone gets NOTIFY messages from the SIP server on the status of the shared phone extension.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone web interface, enter the value in seconds.</li> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;Subscription_Expires_1_ ua="na"&gt;3600&lt;/Subscription_Expires_1_&gt;</pre> </li> </ul> <p>Valid values: An integer from 10 through 65535</p> <p>Default: 3600 seconds</p>
Restrict MWI (Message Waiting Indicator)	<p>Indicates the message waiting indicator lights only for messages on private.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone web interface, select <b>Yes</b> to enable. When enabled the message waiting indicator lights only for messages on private. Otherwise, select <b>No</b>.</li> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;Restrict_MWI_1_ ua="na"&gt;No&lt;/Restrict_MWI_1_&gt;</pre> </li> </ul> <p>Valid values: Yes No</p> <p>Default: No</p>

The following table describes the parameters in the **Voice > Phone** tab of the phone web page.

**Table 21: Miscellaneous Line Key Settings**

Parameter	Description

SCA Barge-In Enable	<p>Enables the SCA Barge-In.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>• In the phone web interface, select <b>Yes</b> to enable. Otherwise, select <b>No</b>.</li> <li>• In the phone configuration file with XML(cfg.xml), enter a string in this format:</li> </ul> <pre>&lt;SCA_Barge-In-Enable ua="na"&gt;No&lt;/SCA_Barge-In-Enable&gt;</pre> <p>Valid values: Yes No</p> <p>Default: No</p>
---------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## Add Dialog-Based Shared Line Appearance

You can now enable dialog-based shared line, so that the phones in the shared line can subscribe to the dialog event package.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

- 
- Step 1** Select **Voice > SIP**.
- Step 2** In the **SIP Parameters** section, set the **Share Line Event Package Type** parameter to **Dialog** to subscribe the phone to the dialog event package.
- You can also set the parameter to **Call-Info** and the phone retains the legacy behavior.
- Default value: **Call-Info**
- You can also configure this parameter in the configuration file (cfg.xml) by entering a string in this format:
- ```
<Share_Line_Event_Package_Type ua="na">Dialog</Share_Line_Event_Package_Type>
```
- Step 3** Click **Submit All Changes**.
- 

## Assign a Ringtone to an Extension

You can also configure the parameters in the phone configuration file with XML (cfg.xml) code. To configure each parameter, see the syntax of the string in [Parameters for Ringtone, on page 169](#).

### Before you begin

[Access the Phone Web Interface, on page 100](#).

## Procedure

- Step 1** Select **Voice > Ext(n)**, where **(n)** is the number of a phone extension.
- Step 2** In the **Call Feature Settings** section, select the **Default Ring** parameter from the list or select no ring. You can also configure this parameter in the configuration file (cfg.xml) by entering a string in this format:
- ```
<Default_Ring_3_ ua="rw">1</Default_Ring_3_>
```
- Step 3** Select **Voice > Phone**.
- Step 4** In the **Ringtone** section, set the **Ring(n)** and **Silent Ring Duration** parameters as described in the [Parameters for Ringtone, on page 169](#) table.
- Step 5** Click **Submit All Changes**.

## Parameters for Ringtone

The following table describes the parameters for **Ringtone**.

**Table 22: Parameters for Ringtone**

Parameter	Description
Ring1 to Ring12	<p>Ring tone scripts for various ringtones.</p> <p>In the phone configuration XML file (cfg.xml), enter a string in this format:</p> <pre>&lt;!-- Ringtone --&gt; &lt;Ring1 ua="na"&gt;n=Sunrise;w=file://Sunrise.rwb;c=1&lt;/Ring1&gt; &lt;Ring2 ua="na"&gt;n=Chirp 1;w=file://chirp1.raw;c=1&lt;/Ring2&gt; &lt;Ring3 ua="na"&gt;n=Chirp 2;w=file://chirp2.raw;c=1&lt;/Ring3&gt; &lt;Ring4 ua="na"&gt;n=Delight;w=file://Delight.rwb;c=1&lt;/Ring4&gt; &lt;Ring5 ua="na"&gt;n=Evolve;w=file://Evolve.rwb;c=1&lt;/Ring5&gt; &lt;Ring6 ua="na"&gt;n=Mellow;w=file://Mellow.rwb;c=1&lt;/Ring6&gt; &lt;Ring7 ua="na"&gt;n=Mischief;w=file://Mischief.rwb;c=1&lt;/Ring7&gt; &lt;Ring8 ua="na"&gt;n=Reflections;w=file://Reflections.rwb;c=1&lt;/Ring8&gt; &lt;Ring9 ua="na"&gt;n=Ringer;w=file://Ringer.rwb;c=1&lt;/Ring9&gt; &lt;Ring10 ua="na"&gt;n=Ascent;w=file://Ascent.rwb;c=1&lt;/Ring10&gt; &lt;Ring11 ua="na"&gt;n=Are you there;w=file://AreYouThereF.raw;c=1&lt;/Ring11&gt; &lt;Ring12 ua="na"&gt;n=Chime;w=file://Chime.raw;c=1&lt;/Ring12&gt; &lt;Silent_Ring_Duration ua="na"&gt;60&lt;/Silent_Ring_Duration&gt;</pre>

Parameter	Description
Silent Ring Duration	<p>Controls the duration of the silent ring. For example, if the parameter is set to 20 seconds, the phone plays the silent ring for 20 seconds then sends 480 response to INVITE message.</p> <p>In the phone configuration XML file (cfg.xml), enter a string in this format: <code>&lt;Ring1 ua="na"&gt;n=Sunrise,w=file://Sunrise.rwb;c=1&lt;/Ring1&gt;</code></p> <p><code>&lt;Silent_Ring_Duration ua="na"&gt;60&lt;/Silent_Ring_Duration&gt;</code></p>

## Add Distinctive Ringtone

You can configure the characteristics of each ring tone using a ring tone script. When the phone receives SIP Alert-INFO message and the message format is correct, then the phone plays the specified ringtone. Otherwise, the phone plays the default ringtone.

### Procedure

In a ring tone script, assign a name for the ring tone and add the script to configure a distinctive ringtone in the format:

```
n=ring-tone-name;h=hint;w=waveform-id-or-path;c=cadence-id;b=break-time;t=total-time
```

where:

**n** = ring-tone-name that identifies this ring tone. This name appears on the Ring Tone menu of the phone. The same name can be used in a SIP Alert-Info header in an inbound INVITE request to tell the phone to play the corresponding ring tone. The name should contain the same characters allowed in a URL only.

**h** = hint used to SIP Alert-INFO rule.

**w** = waveform-id-or-path which is the index of the desired waveform to use in this ring tone. The built-in waveforms are:

- 1 = Classic phone with mechanical bell
- 2 = Typical phone ring
- 3 = Classic ring tone
- 4 = Wide-band frequency sweep signal

**c** = is the index of the desired cadence to play the given waveform. 8 cadences (1–8) as defined in `<Cadence 1>` through `<Cadence 8>`. Cadence-id can be 0 If w=3,4. Setting c=0 implies the on-time is the natural length of the ring tone file.

**b** = break-time that specifies the number of seconds to break between two bursts of ring tone, such as b=2.5.

**t** = total-time that specifies the total number of seconds to play the ring tone before it times out.

In the phone configuration XML file (cfg.xml), enter a string in this format:

```

<!-- Ringtone -->
<Ring1 ua="na">n=Sunrise;w=file://Sunrise.rwb;c=1</Ring1>
<Ring2 ua="na">n=Chirp 1;w=file://chirp1.raw;c=1</Ring2>
<Ring3 ua="na">n=Chirp 2;w=file://chirp2.raw;c=1</Ring3>
<Ring4 ua="na">n=Delight;w=file://Delight.rwb;c=1</Ring4>
<Ring5 ua="na">n=Evolve;w=file://Evolve.rwb;c=1</Ring5>
<Ring6 ua="na">n=Mellow;w=file://Mellow.rwb;c=1</Ring6>
<Ring7 ua="na">n=Mischief;w=file://Mischief.rwb;c=1</Ring7>
<Ring8 ua="na">n=Reflections;w=file://Reflections.rwb;c=1</Ring8>
<Ring9 ua="na">n=Ringer;w=file://Ringer.rwb;c=1</Ring9>
<Ring10 ua="na">n=Ascent;w=file://Ascent.rwb;c=1</Ring10>
<Ring11 ua="na">n=Are you there;w=file://AreYouThereF.raw;c=1</Ring11>
<Ring12 ua="na">n=Chime;w=file://Chime.raw;c=1</Ring12>
<Silent_Ring_Duration ua="na">60</Silent_Ring_Duration>

```

## Enable Hoteling on a Phone

When you enable the hoteling feature of BroadSoft on the phone, the user can sign in to the phone as a guest. After the guest sign out of the phone, the user will switch back to the host user.

You can also configure the parameters in the phone configuration file with XML (cfg.xml) code.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

- 
- Step 1** Select **Voice > Ext [n]** (where [n] is the extension number).
- Step 2** In the **Call Feature Settings** section, set **Enable Broadsoft Hoteling** parameter to **Yes**.
- You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:
- ```
<Enable_Broadsoft_Hoteling_1_ua="na">Yes</Enable_Broadsoft_Hoteling_1>
```
- Options: Yes and No
- Default: No
- Step 3** Set the amount of time (in seconds) that the user can be signed in as a guest on the phone in **Hoteling Subscription Expires**.
- You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:
- ```
<Hoteling_Subscription_Expires_1_ua="na">3600</Hoteling_Subscription_Expires_1>
```
- Valid values: An integer from 10 through 86400
- Default: 3600
- Step 4** Click **Submit All Changes**.
-

## Enable Flexible Seating on a Phone

With the Flexible Seating feature of BroadSoft, the phone downloads and is reconfigured with Flexible Seating Guest's device files when the guest is associated with the host. The phone is treated as an alternate device of the guest. The call originations from guest's primary device are also allowed. The guest's primary device is also alerted on incoming calls to the guest. For more information, see the BroadSoft documentation.

In addition, with the feature enabled on the phone, the phone can cache the user credentials for the LDAP directory. If the cache contains the user credentials, the guest user can bypass the sign-in procedure to access the LDAP directory. The cache can store up to 50 user credentials. The phone removes the least-used credentials when the cache size limit is reached.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

---

**Step 1** Select **Voice > Ext [n]** (where [n] is the extension number).

**Step 2** In the **Call Feature Settings** section, set **Enable Broadsoft Hoteling** parameter to **Yes**.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<Enable_Broadsoft_Hoteling_1_ua="na">Yes</Enable_Broadsoft_Hoteling_1>
```

Options: Yes and No

Default: No

**Step 3** Click **Submit All Changes**.

---

## Enable Extension Mobility on a Phone

With the Extension Mobility (EM) feature enabled on the phone, any user can sign in to the phone other than their own in the same network. In this scenario, the phone can be shared with other users. After the users sign in, they can see their own line number displayed on the phone screen, and their contacts in the personal address directory.

In addition, the phone can cache the user credentials for the LDAP directory when the user signs into the phone with the feature. If the cache contains the user credentials, the user can bypass the sign-in procedure to access the LDAP directory. The cache can store up to 50 user credentials. The phone removes the least-used credentials when the cache size limit is reached.

You can also configure the parameters in the phone configuration file with XML (cfg.xml) code.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

## Procedure

---

- Step 1** Select **Voice > Phone**.
- Step 2** In the **Extension Mobility** section, set **EM Enable** to **Yes**.
- You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:
- ```
<EM_Enable ua="na">Yes</EM_Enable>
```
- Options: Yes and No
- Default: No
- Step 3** Set the amount of time (in minutes) that the user can be signed in on the phone in **Session Timer(m)**.
- You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:
- ```
<Session_Timer_m_ ua="na">480</Session_Timer_m_>
```
- Default: 480
- Step 4** Click **Submit All Changes**.
- 

# Set the User Password

Configure a password so the phone is protected and secured. Both administrators and users can configure a password and control access to the phone.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code.

## Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

## Procedure

---

- Step 1** Select **Voice > System**.
- Step 2** Under the section **System Configuration**, locate the parameter **User Password**, and click **Change Password** next to the parameter.
- Step 3** Enter the current user password in the **Old Password** field.
- If you don't have a password, keep the field empty.
- Step 4** Enter a new password in the **New Password** field.
- Step 5** Click **Submit**.

The message `Password has been changed successfully.` will display in the web page. The web page will refresh in several seconds.

After you set the user password, this parameter displays the following in the phone configuration XML file (cfg.xml):

```
<!--
  <User_Password ua="rw">*****</User_Password>
-->
```

## Download Problem Reporting Tool Logs

Users submit problem reports to you with the Problem Reporting Tool.

If you are working with Cisco TAC to troubleshoot a problem, they typically require the logs from the Problem Reporting Tool to help resolve the issue.

To issue a problem report, users access the Problem Reporting Tool and provide the date and time that the problem occurred, and a description of the problem. You need to download the problem report from the Configuration Utility page.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

- 
- Step 1** Select **Info > Debug Info > Device Logs**.
  - Step 2** In the **Problem Reports** area, click the problem report file to download.
  - Step 3** Save the file to your local system and open the file to access the problem reporting logs.
- 

## Configure Problem Report Tool

You must use a server with an upload script to receive the problem reports that the user sends from the phone.

- If the URL specified in the **PRT Upload Rule** field is valid, users get a notification alert on the phone UI saying that they have successfully submitted the problem report.
- If the **PRT Upload Rule** field is empty or has an invalid URL, users get a notification alert on the phone UI saying that the data upload failed.

The phone uses an HTTP/HTTPS POST mechanism, with parameters similar to an HTTP form-based upload. The following parameters are included in the upload (utilizing multipart MIME encoding):

- devicename (example: "SEP001122334455")
- serialno (example: "FCH12345ABC")
- username (The user name is either the **Station Display Name** or the **User ID** of the extension. The **Station Display Name** is first considered. If this field is empty, then the **User ID** is chosen.)



- prt\_file (example: "probrep-20141021-162840.tar.gz")

You can generate PRT automatically at specific intervals and can define the PRT file name.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code. To configure each parameter, see the syntax of the string in the [Parameters for Configure Problem Report Tool, on page 176](#) table.

A sample script is shown below. This script is provided for reference only. Cisco does not provide support for the upload script installed on a customer's server.

```
<?php
// NOTE: you may need to edit your php.ini file to allow larger
// size file uploads to work.
// Modify the setting for upload_max_filesize
// I used: upload_max_filesize = 20M

// Retrieve the name of the uploaded file
$filename = basename($_FILES['prt_file']['name']);

// Get rid of quotes around the device name, serial number and username if they exist
$devicename = $_POST['devicename'];
$devicename = trim($devicename, "\"");

$serialno = $_POST['serialno'];
$serialno = trim($serialno, "\"");

$username = $_POST['username'];
$username = trim($username, "\"");

// where to put the file
$fullfilename = "/var/prtuploads/".$filename;

// If the file upload is unsuccessful, return a 500 error and
// inform the user to try again

if(!move_uploaded_file($_FILES['prt_file']['tmp_name'], $fullfilename)) {
    header("HTTP/1.0 500 Internal Server Error");
    die("Error: You must select a file to upload.");
}

?>
```

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

- 
- Step 1** Select **Voice > Provisioning**.
  - Step 2** In the **Problem Report Tool** section, set the fields as described in the [Parameters for Configure Problem Report Tool, on page 176](#) table.
  - Step 3** Click **Submit All Changes**.
-

## Parameters for Configure Problem Report Tool

The following table defines the function and usage of Configure Problem Report Tool parameters in the Problem Report Tool section under the Voice > Provisioning tab in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file with XML(cfg.xml) code to configure a parameter.

**Table 23: Parameters for Configure Problem Report Tool**

Parameter	Description
PRT Upload Rule	<p>Specifies the path to the PRT upload script.</p> <p>If the <b>PRT Max Timer</b> and <b>PRT Upload Rule</b> fields are empty, the phone doesn't generate the problem reports automatically unless user manually performs the generation.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;PRT_Upload_Rule ua="na"&gt;https://proxy.example.com/prt_upload.php&lt;/PRT_Upload_Rule&gt;</pre> </li> <li>In the phone web page, enter the path in the format: <pre>https://proxy.example.com/prt_upload.php</pre> <p>or</p> <pre>http://proxy.example.com/prt_upload.php</pre> </li> </ul> <p>Default: Empty</p>
PRT Upload Method	<p>Determines the method used to upload PRT logs to the remote server.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;PRT_Upload_Method ua="na"&gt;POST&lt;/PRT_Upload_Method&gt;</pre> </li> <li>In the phone web page, select <b>POST</b> or <b>PUT</b> methods to upload the logs to the remote server.</li> </ul> <p>Valid values: POST and PUT</p> <p>Default: POST</p>

Parameter	Description
PRT Max Timer	<p>Determines at what interval (minutes) the phone starts generating problem report automatically.</p> <p>If the <b>PRT Max Timer</b> and <b>PRT Upload Rule</b> fields are empty, the phone doesn't generate the problem reports automatically unless user manually performs the generation.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;PRT_Max_Timer ua="na"&gt;30&lt;/PRT_Max_Timer&gt;</pre> </li> <li>In the phone web page, enter the interval duration in minutes.</li> </ul> <p>Valid value range: 15 minutes to 1440 minutes</p> <p>Default: Empty</p>
PRT Name	<p>Defines a name for the generated PRT file.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;PRT_Name ua="na"&gt;prt-string1-\$MACRO&lt;/PRT_Name&gt;</pre> <p>Enter the name in the format:</p> <pre>prt-string1-\$MACRO</pre> </li> <li>In the phone web page, enter the name in the format: <pre>prt-string1-\$MACRO</pre> </li> </ul> <p>Default: Empty</p>
PRT HTTP Header	<p>Specifies the HTTP header for the URL in <b>PRT Upload Rule</b>.</p> <p>The parameter value is associated with <b>PRT HTTP Header Value</b>.</p> <p>Only when both parameters are configured, the HTTP header is included in the HTTP request.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;PRT_HTTP_Header ua="na"&gt;x-cisco-spark-canary-opts&lt;/PRT_HTTP_Header&gt;</pre> </li> <li>In the phone web page, enter the HTTP header in the format: <pre>x-cisco-spark-canary-opts</pre> </li> </ul> <p>Valid value range: a-z, A-Z, 0-9, underscore (_), and hyphen (-)</p> <p>Default: Empty</p>

Parameter	Description
PRT HTTP Header Value	<p>Sets the value of the specified HTTP header.</p> <p>The parameter value is associated with <b>PRT HTTP Header</b>.</p> <p>Only when both parameters are configured, the HTTP header is included in the HTTP request.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;PRT_HTTP_Header_Value ua="na"&gt;always&lt;/PRT_HTTP_Header_Value&gt;</pre> </li> <li>In the phone web page, enter the value in the format: <pre>always</pre> </li> </ul> <p>Valid value range: a-z, A-Z, 0-9, underscore (_), comma (,), semicolon (;), equal (=), and hyphen (-)</p> <p><b>Note</b> Except for the underscore (_), the first character must not be a special character.</p> <p>Default: Empty</p>

## Server-Configured Paging

You can configure a paging group on a server so that users can page a group of phones. For more details, refer to your server documentation.

## Configure Multicast Paging

You can set up Multicast paging to allow users to page to phones. The page can go to all phones or a group of phones in the same network. Any phone in the group can initiate a multicast paging session. The page is received only by the phones that are set to listen for the paging group.

You can add a phone to up to 10 paging groups. Each paging group has a unique multicast port and number. The phones within a paging group must subscribe to the same multicast IP address, port, and multicast number.

You configure the priority for the incoming page from a specific group. When a phone is active and an important page must be played, the user hears the page on the active audio path.

When multiple paging sessions occur, they are answered in chronological order. After the active page ends, the next page is automatically answered. When do not disturb (DND) is enabled, the phone ignores any incoming paging.

You can specify a codec for the paging to use. The supported codecs are G711a, G711u, G722, and G729. If you don't specify the codec, paging uses G711u by default.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code. To configure each parameter, see the syntax of the string in [Parameters for Multiple Paging Group, on page 179](#).

**Before you begin**

- Make sure that your network supports multicast so that all devices in the same paging group are able to receive paging.
- Make sure that all the phones in a paging group are in the same network.
- Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

**Procedure**

---

- Step 1** Select **Voice > Phone**.
- Step 2** Go to the **Multiple Paging Group Parameters** section.
- Step 3** Enter multicast paging scripts as defined in [Parameters for Multiple Paging Group, on page 179](#).
- Step 4** Click **Submit All Changes**.
- 

## Parameters for Multiple Paging Group

The following table defines the function and usage of the multiple paging group parameters in the **Voice > Phone** tab in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file (cfg.xml) with XML code to configure a parameter.

*Table 24: Multiple Paging Group Parameters*

Feature	Description
Group 1 Paging Script — Group 10 Paging Script	

Feature	Description
	<p>Enter a string to configure the phone to listen for and initiate multicast paging. You can add a phone to up to 10 paging groups. Enter the script in this format:</p> <pre>pggrp=&lt;multicast-address&gt;:&lt;port&gt;;&lt;name=group_name&gt;;&lt;num=multicast_number&gt;;&lt;listen=boolean_value&gt;;&lt;pri=priority_level&gt;;&lt;codec=codec_name&gt;;</pre> <p><b>Example script:</b></p> <pre>pggrp=224.168.168.168:34560;name=GroupA;num=500;listen=yes;pri=1;codec=g711a;</pre> <ul style="list-style-type: none"> <li>• Multicast IP address (multicast-address) and port (port)—Enter the multicast IP address and the port specified on your paging server. The port number must be unique for each group and an even number within 1000 and 65534.</li> </ul> <p>Make sure that you set the same multicast IP address and port for all the phones within a paging group. Otherwise, the phones can't receive paging.</p> <ul style="list-style-type: none"> <li>• Paging group name (name)—Optionally enter the name of the paging group. The name helps you identify the paging group the phone is in when you have multiple paging groups.</li> <li>• Multicast number (num)—Specify the number for the phone to listen for multicast paging and initiate a multicast paging session. Assign the same multicast number to all the phones within the group. The number must comply to the dial plan specified for the line to initiate a multicast.</li> <li>• Listen status (listen)—Specify whether the phone listens for paging from this group. Set this parameter to <b>yes</b> to make the phone listen for the paging. Otherwise, set it to <b>no</b>, or don't include this parameter in the script.</li> <li>• Priority (pri)—Specify priority between paging and phone call. If you don't specify the priority or don't include this parameter in the script, the phone uses priority <b>1</b>. The four priority levels are: <ul style="list-style-type: none"> <li>• <b>0</b>: Paging takes precedent over phone call. When the phone is on an active call, an incoming paging places the active call on hold. The call resumes when the paging ends.</li> <li>• <b>1</b>: When the phone receives an incoming paging on an active call, the user hears the mix of the paging and the call.</li> <li>• <b>2</b>: The user is alerted with the paging tone when receiving an incoming paging on an active line. The incoming paging isn't answered unless the active call is put on hold or ends.</li> <li>• <b>3</b>: The phone ignores the incoming paging without any alert when the phone is on an active call.</li> </ul> </li> <li>• Audio codec (codec)—Optionally specify the audio codec for the multicast paging to use. The supported codecs are G711a, G711u, G722, and G729. If you don't specify the codec or don't include the codec parameter in the script, the phone uses G711u codec.</li> </ul> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>• In the phone configuration file with XML(cfg.xml), enter a string in this format:</li> </ul>

Feature	Description
	<pre>&lt;Group_1_Paging_Script ua="na"&gt;pggrp=224.168.168.168:34560;name=Group_1; num=800;listen=yes;pri=1;codec=g722&lt;/Group_1_Paging_Script&gt;</pre> <ul style="list-style-type: none"> <li>In the phone web interface, configure this field with a valid string.</li> </ul> <p>Default: Empty</p>

## Configure a Phone to Accept Pages Automatically

The Single Paging or Intercom feature enables a user to directly contact another user by phone. If the phone of the person being paged has been configured to accept pages automatically, the phone does not ring. Instead, a direct connection between the two phones is automatically established when paging is initiated.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

**Step 1** Select **Voice > User**.

**Step 2** In the **Supplementary Services** section, choose **Yes** for the **Auto Answer Page** parameter.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<Auto_Answer_Page ua="na">Yes</Auto_Answer_Page>
```

Options: Yes and No

Default: Yes

**Step 3** Click **Submit All Changes**.

## Manage Phones with TR-069

You can use the protocols and standards defined in Technical Report 069 (TR-069) to manage phones. TR-069 explains the common platform for management of all phones and other customer-premises equipment (CPE) in large-scale deployments. The platform is independent of phone types and manufacturers.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code. To configure each parameter, see the syntax of the string in the [Parameters for TR-069 Configuration, on page 184](#) table.

As a bidirectional SOAP/HTTP-based protocol, TR-069 provides the communication between CPEs and Auto Configuration Servers (ACS).

For TR-069 Enhancements, see [TR-069 Parameter Comparison, on page 467](#).



**Before you begin**

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

**Procedure**

---

- Step 1** Select **Voice > TR-069**.
- Step 2** Set up the fields as described in [Parameters for TR-069 Configuration, on page 184](#) table.
- Step 3** Click **Submit All Changes**.
- 

## View TR-069 Status

When you enable TR-069 on a user phone, you can view status of TR-069 parameters on the phone web interface.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code. To configure each parameter, see the syntax of the string in the [Parameters for TR-069 Configuration, on page 184](#) table.

**Before you begin**

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

**Procedure**

---

Select **Info > Status > TR-069 Status**.

You can view status of TR-069 parameters in [Parameters for TR-069 Configuration, on page 184](#) table.

---

## Parameters for TR-069 Configuration

The following table defines the function and usage of Call Center Agent Setup parameters in the ACD Settings section under the Ext(n) tab in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file with XML(cfg.xml) code to configure a parameter.

**Table 25: Parameters for TR-069 Configuration**

Parameter	Description
Enable TR-069	<p>Settings that enables or disables the TR-069 function.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:           <pre>&lt;Enable_TR-069 ua="na"&gt;No&lt;/Enable_TR-069&gt;</pre> </li> <li>In the phone web page, select <b>Yes</b> to enable this feature and select <b>No</b> to disable it.</li> </ul> <p>Valid values: Yes No</p> <p>Default: No</p>
ACS URL	<p>URL of the ACS that uses the CPE WAN Management Protocol. This parameter must be in the form of a valid HTTP or HTTPS URL. The host portion of this URL is used by the CPE to validate the ACS certificate when it uses SSL or TLS.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:           <pre>&lt;ACS_URL ua="na"&gt;https://acs.url.com&lt;/ACS_URL&gt;</pre> </li> <li>In the phone web page, enter a valid HTTP or HTTPS URL of the ACS.</li> </ul> <p>Default: Blank</p>
ACS Username	<p>Username that authenticates the CPE to the ACS when ACS uses the CPE WAN Management Protocol. This username is used only for HTTP-based authentication of the CPE.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:           <pre>&lt;ACS_Username ua="na"&gt;acs username&lt;/ACS_Username&gt;</pre> </li> <li>In the phone web page, enter a valid username for HTTPS-based authentication of the CPE.</li> </ul> <p>Default: admin</p>

Parameter	Description
ACS Password	<p>Password to access to the ACS for a specific user. This password is used only for HTTP-based authentication of the CPE.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;ACS_Password ua="na"/&gt;</pre> </li> <li>In the phone web page, enter a valid password for HTTPS-based authentication of the CPE.</li> </ul> <p>Default: Blank</p>
ACS URL In Use	URL of the ACS that is currently in use. This is a read-only field.
Connection Request URL	This is read-only field showing the URL of the ACS that makes the connection request to the CPE.
Connection Request Username	<p>Username that authenticates the ACS that makes the connection request to the CPE.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;Connection_Request_Password ua="na"/&gt;</pre> </li> <li>In the phone web page, enter a valid username that authenticates the ACS.</li> </ul>
Connection Request Password	<p>Password used to authenticate the ACS that makes a connection request to the CPE.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;Connection_Request_Password ua="na"/&gt;</pre> </li> <li>In the phone web page, enter a valid password that authenticates the ACS.</li> </ul> <p>Default: Blank</p>

Parameter	Description
Periodic Inform Interval	<p>Duration in seconds of the interval between CPE attempts to connect to the ACS when Periodic Inform Enable is set to yes.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;Periodic_Inform_Interval ua="na"&gt;20&lt;/Periodic_Inform_Interval&gt;</pre> </li> <li>In the phone web page, enter a valid duration in seconds.</li> </ul> <p>Default: 20</p>
Periodic Inform Enable	<p>Settings that enables or disables the CPE connection requests.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;Periodic_Inform_Enable ua="na"&gt;Yes&lt;/Periodic_Inform_Enable&gt;</pre> </li> <li>In the phone web page, select <b>Yes</b> to enable this feature and select <b>No</b> to disable it.</li> </ul> <p>Valid values: Yes No</p> <p>Default: Yes</p>
TR-069 Traceability	<p>Settings that enables or disables TR-069 transaction logs.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;TR-069_Traceability ua="na"&gt;Yes&lt;/TR-069_Traceability&gt;</pre> </li> <li>In the phone web page, select <b>Yes</b> to enable this feature and select <b>No</b> to disable it.</li> </ul> <p>Valid values: Yes No</p> <p>Default: No</p>

Parameter	Description
CWMP V1.2 Support	<p>Settings that enables or disables CPE WAN Management Protocol (CWMP) support. If set to disable, the phone does not send any Inform messages to the ACS nor accept any connection requests from the ACS.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:   <pre>&lt;CWMP_V1.2_Support ua="na"&gt;Yes&lt;/CWMP_V1.2_Support&gt;</pre> </li> <li>In the phone web page, select <b>Yes</b> to enable this feature and select <b>No</b> to disable it.</li> </ul> <p>Valid values: Yes No Default: Yes</p>
TR-069 VoiceObject Init	<p>Settings to modify voice objects.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:   <pre>&lt;TR-069_VoiceObject_Init ua="na"&gt;Yes&lt;/TR-069_VoiceObject_Init&gt;</pre> </li> <li>In the phone web page, select <b>Yes</b> to initialize all voice objects to factory default values or select <b>No</b> to retain the current values.</li> </ul> <p>Valid values: Yes No Default: Yes</p>
TR-069 DHCPOption Init	<p>Settings to modify DHCP settings.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:   <pre>&lt;TR-069_DHCPOption_Init ua="na"&gt;Yes&lt;/TR-069_DHCPOption_Init&gt;</pre> </li> <li>In the phone web page, select <b>Yes</b> to initialize the DHCP settings from the ACS or select <b>No</b> to retain the current DHCP settings.</li> </ul> <p>Valid values: Yes No Default: Yes</p>

Parameter	Description
BACKUP ACS URL	<p>Backup URL of the ACS that uses the CPE WAN Management Protocol. This parameter must be in the form of a valid HTTP or HTTPS URL. The host portion of this URL is used by the CPE to validate the ACS certificate when it uses SSL or TLS.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;BACKUP_ACS_URL ua="na"&gt;https://acs.url.com&lt;/BACKUP_ACS_URL&gt;</pre> </li> <li>In the phone web page, enter a valid URL that uses the CPE WAN Management Protocol.</li> </ul> <p>Default: Blank</p>
BACKUP ACS User	<p>Backup username that authenticates the CPE to the ACS when ACS uses the CPE WAN Management Protocol. This username is used only for HTTP-based authentication of the CPE.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;BACKUP_ACS_User ua="na"&gt;backup username&lt;/BACKUP_ACS_User&gt;</pre> </li> <li>In the phone web page, enter a valid username that authenticates the CPE to the ACS when ACS uses the CPE WAN Management Protocol.</li> </ul> <p>Default: Blank</p>
BACKUP ACS Password	<p>Backup password to access to the ACS for a specific user. This password is used only for HTTP-based authentication of the CPE.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;BACKUP_ACS_Password ua="na"/&gt;</pre> </li> <li>In the phone web page, enter a valid password that authenticates the CPE to the ACS when ACS uses the CPE WAN Management Protocol.</li> </ul> <p>Default: Blank</p>
<b>Note</b>	If you do not configure the above parameters, you can also fetch them through DHCP options 60,43, and 125.

# Set up a Secure Extension

You can configure an extension to only accept secure calls. If the extension is configured to only accept secure calls then any calls the extension makes will be secure.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code.

## Before you begin

- Make sure that **Secure Call Serv** is enabled (set to **Yes**) in the **Supplementary Services** area on the **Voice > Phone** tab.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<Secure_Call_Serv ua="na">Yes</Secure_Call_Serv>
```

- SIP transport with TLS can be set statically on the phone web page or automatically with information in the DNS NAPTR records. If the SIP transport parameter is set for the phone extension as TLS, the phone only allows SRTP. If the SIP transport parameter is set to AUTO, the phone performs a DNS query to get the transport method.
- Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

## Procedure

- 
- Step 1** Select **Voice > Ext(n)**.
- Step 2** In the **Call Feature Settings** section, in the **Secure Call Option** field, choose **Optional, Required**, or **Strict**.  
You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:
- ```
<Secure_Call_Option_1_ ua="na">Optional</Secure_Call_Option_1_>
```
- Options: Optional, Required, and Strict
- Optional - Retains the current secure call option for the phone.
  - Required - Rejects nonsecure calls from other phones.
  - Strict - Allows SRTP only when SIP transport is set to **TLS**. Allows RTP only when SIP transport is **UDP/TCP**.
- Default: Optional
- Step 3** Click **Submit All Changes**.
- 

# Configure the SIP Transport

For SIP messages, you can configure each extension to use:

- a specific protocol
- the protocol automatically selected by the phone

When you set up automatic selection, the phone determines the transport protocol based on the Name Authority Pointer (NAPTR) records on the DNS server. The phone uses the protocol with the highest priority in the records.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

- 
- Step 1** Select **Voice > Ext(n)**, where n is an extension number.
- Step 2** In the **SIP Settings** section, set the **SIP Transport** parameter to select a transport protocol for SIP messages. You can configure this parameter in the phone configuration XML file (cfg.xml) with a string in this format:
- ```
<SIP_Transport_n_ ua="na">UDP</SIP_Transport_n_>
```
- where *n* is the extension number.
- Options: UDP, TCP, TLS, and Auto
- AUTO allows the phone to select the appropriate protocol automatically, based on the NAPTR records on the DNS server.
- Default: UDP
- Step 3** Click **Submit All Changes**.
- 

## Block Non-Proxy SIP Messages to a Phone

You can disable the ability of the phone to receive incoming SIP messages from a non-proxy server. When you enable this feature, the phone only accepts SIP messages from:

- proxy server
- outbound proxy server
- alternative proxy server
- alternative outbound proxy server
- IN-Dialog message from proxy server and non-proxy server. For example: Call Session dialog and Subscribe dialog

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code.



**Before you begin**

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

**Procedure**

- 
- Step 1** Select **Voice > System**.
- Step 2** In the **System Configuration** section, set the **Block Nonproxy SIP** parameter to **Yes** to block any incoming non-proxy SIP messages except IN-dialog message. If you choose **No**, the phone does not block any incoming non-proxy SIP messages.
- Set **Block Nonproxy SIP** to **No** for phones that use TCP or TLS to transport SIP messages. Nonproxy SIP messages transported over TCP or TLS are blocked by default.
- You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:
- ```
<Auto_Answer_Page ua="na">Yes</Auto_Answer_Page>
```
- Options: Yes and No
- Default: No
- Step 3** Click **Submit All Changes**.
- 

## Configure a Privacy Header

A user privacy header in the SIP message sets user privacy needs from the trusted network.

You can set the user privacy header value for each line extension.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code.

**Before you begin**

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

**Procedure**

- 
- Step 1** Select **Voice > Extension**.
- Step 2** In the **SIP Settings** section, set the **Privacy Header** parameter to set user privacy in the SIP message in the trusted network.
- You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:
- ```
<Privacy_Header_2_ ua="na">header</Privacy_Header_2_>
```
- Options:
- Disabled (default)
  - none—The user requests that a privacy service applies no privacy functions to this SIP message.

- header—The user needs a privacy service to obscure headers which cannot be purged of identifying information.
- session—The user requests that a privacy service provide anonymity for the sessions.
- user—The user requests a privacy level only by intermediaries.
- id—The user requests that the system substitute an id that doesn't reveal the IP address or host name.

Default: Disabled

**Step 3** Click **Submit All Changes**.

---

## Enable P-Early-Media Support

You can determine whether to include the P-Early-Media header in the SIP message of outgoing calls. The P-Early-Media header contains the status of the early media stream. If the status indicates that the network is blocking the early media stream, the phone plays the local ringback tone. Otherwise, the phone plays the early media while waiting for the call to be connected.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

---

**Step 1** Select **Voice > Ext (n)**.

**Step 2** In the **SIP Settings** section, set the **P-Early-Media Support** to **Yes** to control whether the P-Early-Media header is included in the SIP message for an outgoing call.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<P-Early-Media_Support_1_ua="na">No</P-Early-Media_Support_1_>
```

Options: Yes and No

Default: No

**Step 3** Click **Submit All Changes**.

---

## Enable Peer Firmware Sharing

Peer Firmware Sharing (PFS) is a firmware distribution model which allows a Cisco IP phone to find other phones of the same model or series on the subnet and share updated firmware files when you need to upgrade multiple phones all at the same time. PFS uses Cisco Peer-to-Peer-Distribution Protocol (CPPDP) which is a

Cisco proprietary protocol. With CPPDP, all the devices in the subnet form a peer-to-peer hierarchy, and then copy the firmware or the other files from peer devices to the neighboring devices. To optimize firmware upgrades, a root phone downloads the firmware image from the load server and then transfers the firmware to other phones on the subnet using TCP connections.

Peer firmware sharing:

- Limits congestion on TFTP transfers to centralized remote load servers.
- Eliminates the need to manually control firmware upgrades.
- Reduces phone downtime during upgrades when large numbers of phones are reset simultaneously.



#### Note

- Peer firmware sharing does not function unless multiple phones are set to upgrade at the same time. When a NOTIFY is sent with Event:resync, it initiates a resync on the phone. Example of an xml that can contain the configurations to initiate the upgrade:  

```
“Event:resync;profile=”http://10.77.10.141/profile.xml
```
- When you set the Peer Firmware Sharing Log server to an IP address and port, the PFS specific logs are sent to that server as UDP messages. This setting must be done on each phone. You can then use the log messages when troubleshooting issues related to PFS.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code.

#### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

#### Procedure

**Step 1** Select **Voice > Provisioning**.

**Step 2** In the **Firmware Upgrade** section, set the parameters:

- a) Set the **Peer Firmware Sharing** parameter.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<Peer_Firmware_Sharing ua="na">Yes</Peer_Firmware_Sharing>
```

Options: Yes and No

Default: Yes

- b) Set the **Peer Firmware Sharing Log Server** parameter to indicate the IP address and the port to which the UDP message is sent.

For example: 10.98.76.123:514 where, 10.98.76.123 is the IP address and 514 is the port number.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<Peer_Firmware_Sharing_Log_Server>192.168.5.5</ Peer_Firmware_Sharing_Log_Server>
```

Peer\_Firmware\_Sharing\_Log\_Server specifies UDP Remote syslog server hostname and the port. The port defaults to the default syslog 514.

**Step 3** Click **Submit All Changes**.

---

## Specify the Profile Authentication Type

Profile Authentication allows phone users to resynchronize the provisioning profile onto the phone. Authentication information is required while the phone tries to resynchronize and download configuration file for the first time and gets an HTTP or HTTPS 401 authentication error. When you enable this feature, the **Profile account setup** screen is displayed on the phone for the following situations:

- When the HTTP or HTTPS 401 authentication error occurs during first-time provisioning after the phone reboots
- When the profile account username and password are empty
- When there are no username and password in the Profile Rule

If the **Profile account setup** screen is missed or ignored, the user can also access the setup screen through the phone screen menu, or the **Setup** softkey, which displays only when no line on the phone is registered.

When you disable the feature, the **Profile account setup** screen doesn't display on the phone.

The username and password in the **Profile Rule** field have a higher priority than the profile account.

- When you provide a correct URL in the **Profile Rule** field without a username and password, the phone requires authentication or digest to resynchronize the profile. With the correct profile account, authentication passes. With an incorrect profile account, authentication fails.
- When you provide a correct URL in the **Profile Rule** field with a correct username and password, the phone requires authentication or digest to resynchronize the profile. The profile account is not used for phone resynchronization. Sign-in is successful.
- When you provide a correct URL in the **Profile Rule** field with an incorrect username and password, the phone requires authentication or digest to resynchronize the profile. The profile account isn't used for phone resynchronization. Sign-in always fails.
- When you provide an incorrect URL in the **Profile Rule** field, sign-in always fails.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code.

You can specify the profile authentication type from the phone administration web page.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

---

**Step 1** Select **Voice > Provisioning**.

**Step 2** In the **Configuration Profile** section, set the **Profile Authentication Type** parameter to specify the credentials to use for profile account authentication.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<Profile_Authentication_Type ua="na">Disabled</Profile_Authentication_Type>
```

Options:

- **Disabled:** Disables the profile account feature. When this feature is disabled, the **Profile account setup** menu doesn't display on the phone screen.
- **Basic HTTP Authentication:** The HTTP login credentials are used to authenticate the profile account.
- **XSI Authentication:** XSI login credentials or XSI SIP credentials are used to authenticate the profile account. The authentication credentials depend on the XSI Authentication Type for the phone:

When the XSI Authentication Type for the phone is set to Login Credentials, the XSI login credentials are used.

When the XSI Authentication Type for the phone is set to SIP Credentials, the XSI SIP credentials are used.

Default: Basic HTTP Authentication

**Step 3** Click **Submit All Changes**.

---

## Control the Authentication Requirement to Access the Phone Menus

You can control if authentication is required to access phone menus.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

---

**Step 1** Select **Voice > Phone**.

**Step 2** Set the **LCD Authentication** and **LCD Authentication Customization** sections as described in the [Parameters for User Authentication Control, on page 195](#) table.

---

## Parameters for User Authentication Control

The following table defines the function and usage of the parameters for user authentication control feature in the **LCD Authentication** and **LCD Authentication Customization** section under the **Voice > Phone** tab

in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file (cfg.xml) with XML code to configure a parameter.

**Table 26: Parameters for User Authentication Control**

Parameter	Description
Require Authentication for LCD Menu Access	<p>Controls whether the user requires authentication to access phone menus.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;Require_Authentication_for_LCD_Menu_Access ua="na"&gt;Default&lt;/Require_Authentication_for_LCD_Menu_Access&gt;</pre> </li> <li>On the phone web interface, select the required value.</li> </ul> <p>Allowed values: Default Customized No</p> <ul style="list-style-type: none"> <li><b>Default</b>—When selected, user needs to provide password and then sign in to access the phone menus that requires authentication. Phone continues to support all the functionalities that are supported in the releases prior to 11.3(2). Phone displays lock screen icon. <p>To access any phone menus that require authentication, user needs to provide the password and press <b>Sign in</b>. The lock icon remains locked. After the user signs in, the lock icon is unlocked.</p> </li> <li><b>Customized</b>—When selected, user requires authentication only to access <b>Profile rule</b> and <b>Factory reset</b> menus on the phone. Authentication control of these two menus also depends on the settings of the <b>Factory Reset Menu</b> menu and the <b>Profile Rule Menu</b> menu. User will not require any authentication to access other phone menus.</li> <li><b>No</b>—When selected, the <b>Sign in</b> menu, the <b>Sign out</b> menu, the lock icon, and the <b>Set password</b> menus are not available on the phone. User can access phone menus without any authentication.</li> </ul> <p>Default value: Default</p>
Factory Reset Menu	<p>Specifies if the user requires authentication to access <b>Factory reset</b> menu on the phone. You can customize this parameter to <b>Yes</b> or <b>No</b> only when you set the <b>Require Authentication for LCD Menu Access</b> parameter to <b>Customized</b>.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;Factory_Reset_Menu ua="na"&gt;Yes&lt;/Factory_Reset_Menu&gt;</pre> </li> <li>On the phone web interface, set this parameter to <b>Yes</b> or <b>No</b> as needed.</li> </ul> <p>Allowed values: Yes No</p> <p>Default value: Yes</p>

Parameter	Description
Profile Rule Menu	<p>Specifies if the user requires authentication to access <b>Profile rule</b> menu on the phone.</p> <p>You can customize this parameter to <b>Yes</b> or <b>No</b> only when you set the <b>Require Authentication for LCD Menu Access</b> parameter to <b>Customized</b>.</p> <p>Perform one of the following:</p> <pre>&lt;Profile_Rule_Menu ua="na"&gt;Yes&lt;/Profile_Rule_Menu&gt;</pre> <ul style="list-style-type: none"> <li>On the phone web interface, set this parameter to <b>Yes</b> or <b>No</b> as needed.</li> </ul> <p>Allowed values: Yes No</p> <p>Default value: Yes</p>

## Silence an Incoming Call with Ignore Soft Key

You can add the **Ignore** softkey on the phone. User can press this softkey to silence an incoming call when busy and don't want to be disturbed. When the user presses the softkey, the phone stops ringing, but the user gets a visual alert, and, can answer the phone call.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

- 
- Step 1** Select **Voice > Phone**.
- Step 2** In the **Programmable Softkeys** section, set the **Programmable Softkey Enable** to **Yes**.
- Step 3** Enter the following values in the **Ringling Key List** field:
- ```
answer|1;ignore|2;ignoresilent|3;
```
- Step 4** Click **Submit All Changes**.
- 

## Move an Active Call from a Phone to Other Phones (Locations)

You can configure a phone to allow a call to seamlessly be moved from one desk phone(location) to another mobile phone or desk phone(location).

When you enable this feature, the **Anywhere** menu is added into the phone screen. The user can use this menu to add multiple phones as locations to the extension. When there is an incoming call in that extension, all the added phones will ring and the user can answer the incoming call from any location. The locations list also gets saved to the BroadWorks XSI server.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code. To configure each parameter, see the syntax of the string in the [Parameters for Moving Active Call to Other Locations, on page 199](#) table.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

---

- Step 1** Select **Voice > Ext(n)**.
- Step 2** In the **XSI Line Service** section, set the **XSI Host Server**, **XSI Authentication Type**, **Login User ID**, **Login Password**, and **Anywhere Enable** parameters as described in the [Parameters for Moving Active Call to Other Locations, on page 199](#) table.
- If you select **SIP Credentials** for **XSI Authentication Type**, you need to enter subscriber **Auth ID** and **Password** in the **Subscriber Information** section.
- Step 3** Click **Submit All Changes**.
-



## Parameters for Moving Active Call to Other Locations

The following table defines the function and usage of Moving Active Call to Locations parameters in the XSI Line Service section under the Ext(n) tab in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file with XML(cfg.xml) code to configure a parameter.

**Table 27: Parameters for Moving Active Call to Locations**

| Parameter       | Description  |
|-----------------|--|
| XSI Host Server | <p>Enter the name of the server. For example:</p> <pre>xsi.iopl.broadworks.net</pre> <p><b>Note</b> XSI Host Server uses http protocol by default. To enable XSI over HTTPS, you can specify https:// in the server.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:</li> </ul> <pre>&lt;XSI_Host_Server ua="na"&gt;https://xsi.iopl.broadworks.net&lt;/XSI_Host_Server&gt;</pre> <ul style="list-style-type: none"> <li>In the phone web page, enter the server.</li> </ul> <p>For example:</p> <pre>https://xsi.iopl.broadworks.net</pre> <p>You can also specify a port for the server. For example:</p> <pre>https://xsi.iopl.broadworks.net:5061</pre> <p>If you don't specify a port. The default port for the specified protocol is used.</p> <p>Default: Blank</p> |

| Parameter               | Description   |
|-------------------------|---|
| XSI Authentication Type | <p>Determines the XSI authentication type.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;XSI_Authentication_Type ua="na"&gt;SIP Credentials&lt;/XSI_Authentication_Type&gt;</pre> </li> <li>In the phone web page, select an authentication type.</li> </ul> <p>Options:</p> <p>Login Credentials - authenticates access with Login User ID and Login Password.</p> <p>SIP Credentials - authenticates access with the register Auth ID and Password of the SIP account registered on the phone.</p> <p>If you select <b>SIP Credentials</b> for <b>XSI Authentication Type</b>, you need to enter subscriber <b>Auth ID</b> and <b>Password</b> in the <b>Subscriber Information</b> section.</p> <p>Default: Login Credentials</p> |
| Login User ID           | <p>BroadSoft User ID of the phone user.</p> <p>For example:</p> <pre>john.doe@xdp.broadsoft.com.</pre> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;Login_User_ID ua="na"&gt;4081005300@as1bsoft22.sipurash.com&lt;/Login_User_ID&gt;</pre> </li> <li>In the phone web page, enter a valid user ID.</li> </ul> <p>For any XSI Authentication Type, you must enter <b>Login User ID</b>. The BroadWorks Anywhere feature does not work without this parameter.</p> <p>Default: admin</p>   |
| Login Password          | <p>Alphanumeric password associated with the Login User ID.</p> <p>Enter Login Password, when you select <b>Login Credentials</b> for XSI authentication type.</p> <p>After you enter the password, this parameter shows the following in the configuration file (cfg.xml):</p> <pre>&lt;ACS_Password ua="na"&gt;*****&lt;/ACS_Password&gt;</pre> <p>Default: Blank</p>   |

| Parameter       | Description  |
|-----------------|--|
| Anywhere Enable | <p>Enables BroadWorks Anywhere feature on an extension.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;Anywhere_Enable_1_ ua="na"&gt;Yes&lt;/Anywhere_Enable_1_&gt;</pre> </li> <li>In the phone web page, select <b>Yes</b>, Anywhere is enabled on this line, and the user can use the phone menu to add multiple locations to this specific line.</li> </ul> <p>Valid values: Yes No<br/>Default: Yes</p> |

## Sync the Block Caller ID Feature with the Phone and the BroadWorks XSI Server

You can sync the **Block caller id** status on the phone and the **Line ID Blocking** status on the BroadWorks XSI server. When you enable the synchronization, the changes that the user makes in the **Block caller id** settings also changes the BroadWorks server settings.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

**Step 1** Select **Voice > Ext(n)**.

**Step 2** In the **XSI Line Service** section, set the **Block CID Enable** parameter. Choose **Yes** to enable the synchronization of blocking caller id status with the server using XSI interface. Choose **No** to use the phone's local blocking caller id settings.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<Block_CID_Enable_1_ ua="na">No</Block_CID_Enable_1_>
```

- Note**
- When **Feature Key Sync** is set to **Yes**, FKS takes precedent over XSI synchronization.
  - If XSI host server and credentials are not entered and the **CFWD Enable** field is set to **Yes**, the phone user can't forward calls on the phone.

Options: Yes and No

Default: No

**Step 3** Click **Submit All Changes**.

---

## Enable Viewing BroadWorks XSI Call Logs on a Line

You can configure a phone to display recent call logs from either the BroadWorks server or the local phone. After you enable the feature, the Recents screen has a **Display recents from** menu and the user can choose the XSI call logs or the local call logs.

You can set up a feature to do a reverse name lookup against local contacts for BroadWorks server call logs. For example, on server you set up a user 3280 (4085273280) with name "cx400 liu" and another user 3281(4085273281) with name "cx401 liu". User 3280 is registered on phone A and user 3281 is registered on phone B. From phone A you make a missed call, a received call, or a placed call on phone B. The display of the broadsoft call logs on phone B appears as follows:

- If the personal directory doesn't have a contact that matches with the caller name, the BroadWorks call logs on phone B displays the original name "cx400 liu" saved in the server as the caller name.
- If the personal directory has a contact with "Name" = "B3280" and "Work" = "3280" that matches with the calling number, the BroadWorks call logs on phone B displays the contact name "B3280" as the caller name.
- If the personal directory has a contact with "Name" = "C3280" and "Work" = "03280", and the user configures a caller id map rule (<3:03>x.), the BroadWorks call logs on the phone B displays "C3280" using the mapped phone number 03280. If there is a matched contact of the unmapped phone number, the mapped phone number will not be used for reverse name lookup.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code. To configure each parameter, see the syntax of the string in the [Parameters for BroadWorks XSI Call Logs on a Line, on page 203](#) table.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

**CallLog Enable** field is enabled.

### Procedure

---

**Step 1** Select **Voice > Phone**.

**Step 2** In the **XSI Phone Service** section, set the **XSI Host Server**, **XSI Authentication Type**, **Login User ID**, **Login Password**, and **Directory Enable** fields as described in [Parameters for BroadWorks XSI Call Logs on a Line, on page 203](#).

If you select **SIP Credentials** for **XSI Authentication Type**, you need to enter **SIP Auth ID** and **SIP Password** in this section.

**Step 3** Set the **CallLog Associated Line** and **Display Recents From** fields as described in [Parameters for BroadWorks XSI Call Logs on a Line, on page 203](#).

**Note** The **Display recents from** menu doesn't appear in the **Recents** phone screen when you set the value of the **CallLog Enable** field to **No**,

**Step 4** Click **Submit All Changes**.

## Parameters for BroadWorks XSI Call Logs on a Line

The following table defines the function and usage of XSI Call Logs on a Line parameters in the XSI Phone Service section under the Phone tab in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file with XML(cfg.xml) code to configure a parameter.

**Table 28: Parameters for XSI Call Logs on a Line**

| Parameter               | Description   |
|-------------------------|---|
| XSI Host Server         | <p>Enter the name of the server; for example, <code>xsi.iopl.broadworks.net</code>.</p> <p><b>Note</b> XSI Host Server uses http protocol by default. To enable XSI over HTTPS, you can specify <code>https://</code> in the server.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:           <pre>&lt;XSI_Host_Server ua="na"&gt;https://xsi.iopl.broadworks.net&lt;/XSI_Host_Server&gt;</pre> </li> <li>In the phone web interface, enter the XSI server to use.</li> </ul> <p>Default: Empty</p>   |
| XSI Authentication Type | <p>Determines the XSI authentication type. Select <b>Login Credentials</b> to authenticate access with XSI id and password. Select <b>SIP Credentials</b> to authenticate access with the register user ID and password of the SIP account registered on the phone.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:           <pre>&lt;XSI_Authentication_Type ua="na"&gt;SIP Credentials&lt;/XSI_Authentication_Type&gt;</pre> </li> <li>In the phone web interface, specify the authentication type for XSI service.</li> </ul> <p>Options: SIP Credentials and Login Credentials<br/>Default: Login Credentials</p> |

| Parameter        | Description   |
|------------------|---|
| Login User ID    | <p>BroadSoft User ID of the phone user; for example, johndoe@xdp.broadsoft.com.</p> <p>Enter SIP Auth ID when you select <b>Login Credentials</b> or <b>SIP Credentials</b> for XSI authentication type.</p> <p>When you choose SIP Auth ID as <b>SIP Credentials</b>, you must enter Login User ID. Without Login User ID, the BroadSoft directory will not appear under the phone Directory list.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="971 674 1385 722">&lt;Login_User_ID ua="na"&gt;username&lt;/Login_User_ID&gt;</pre> </li> <li>In the phone web interface, enter the username used to authenticate the access to the XSI server.</li> </ul> <p>Default: Empty</p> |
| Login Password   | <p>Alphanumeric password associated with the User ID.</p> <p>Enter login password, when you select <b>Login Credentials</b> for XSI authentication type.</p> <p>Default: Empty</p>  |
| Directory Enable | <p>Enables BroadSoft directory for the phone user. Select <b>Yes</b> to enable the directory and select <b>No</b> to disable it.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="971 1318 1360 1367">&lt;Directory_Enable ua="na"&gt;Yes&lt;/Directory_Enable&gt;</pre> </li> <li>In the phone web interface, set this field to <b>Yes</b> to enable the BroadSoft directory.</li> </ul> <p>Option: Yes and No</p> <p>Default: No</p>   |

| Parameter               | Description   |
|-------------------------|---|
| CallLog Associated Line | <p>Allows you to select a phone line for which you want to display the recent call logs.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;CallLog_Associated_Line ua="na"&gt;1&lt;/CallLog_Associated_Line&gt;</pre> </li> <li>In the phone web interface, Select a phone line.</li> </ul> <p>Valid values: 1 to 10</p> <p>Default: 1</p>   |
| Display Recents From    | <p>Allows you to set which type of recent call logs the phone will display.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;Display_Recents_From ua="na"&gt;Phone&lt;/Display_Recents_From&gt;</pre> </li> <li>In the phone web interface, Choose <b>Server</b> to display BroadSoft XSI recent call logs and select <b>Phone</b> to display local recent call logs.</li> </ul> <p>Option: Phone and Server</p> <p>Default: Phone</p> <p><b>Note</b> The <b>Display recents from</b> is added to the <b>Recents</b> screen of the phone only when you set <b>CallLog Enable</b> to <b>Yes</b> and <b>Display Recents From</b> type to <b>Server</b>.</p> |

## Enable Feature Key Sync

When you enable the Feature Key Synchronization (FKS), the settings of call forward and do not disturb (DND) on the server are synchronized to the phone. The changes in DND and call forward settings made on the phone will also be synchronized to the server.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

## Procedure

- 
- Step 1** Select **Voice > Ext [n]** (where [n] is the extension number).
- Step 2** In the **Call Feature Settings** section, set the **Feature Key Sync** field to **Yes**.
- Step 3** Click **Submit All Changes**.
- 

## Related Topics

- [DND and Call Forward Status Sync](#), on page 206
- [Enable Call Forward Status Sync via XSI Service](#), on page 207
- [Enable DND Status Sync via XSI Service](#), on page 208

# DND and Call Forward Status Sync

You can configure the settings on the phone administration web page to enable status synchronization of do not disturb (DND) and call forward between the phone and the server.



There are two ways to synchronize the feature status:

- Feature Key Synchronization (FKS)
- XSI Synchronization

FKS uses SIP messages to communicate the feature status. XSI Synchronization uses HTTP messages. If both FKS and XSI synchronization are enabled, FKS takes precedent over XSI synchronization. See the table below for how FKS interacts with XSI synchronization.

**Table 29: Interaction Between FKS and XSI Synchronization**

| Feature Key Sync | DND Enabled | CFWD Enabled | DND Sync   | CFWD Sync  |
|------------------|-------------|--------------|------------|------------|
| Yes              | Yes         | Yes          | Yes (SIP)  | Yes (SIP)  |
| Yes              | No          | No           | Yes (SIP)  | Yes (SIP)  |
| Yes              | No          | Yes          | Yes (SIP)  | Yes (SIP)  |
| Yes              | No          | No           | Yes (SIP)  | Yes (SIP)  |
| No               | Yes         | Yes          | Yes (HTTP) | Yes (HTTP) |
| No               | No          | Yes          | No         | Yes (HTTP) |
| No               | Yes         | No           | Yes (HTTP) | No         |
| No               | No          | No           | No         | No         |

If a line key is configured with FKS or XSI synchronization and is also enabled with DND or call forward, the respective DND  icon or the call forward  icon is displayed next to the line key label. If the line key has a missed call, a voice message, or an urgent voicemail alert, the DND icon or the call forward icon is also displayed with the alert notification.



**Related Topics**

- [Enable Feature Key Sync](#), on page 205
- [Enable Call Forward Status Sync via XSI Service](#), on page 207
- [Enable DND Status Sync via XSI Service](#), on page 208

## Enable Call Forward Status Sync via XSI Service

When call forward sync is enabled, the settings related to call forward on the server are synchronized to the phone. The changes in call forward settings made on the phone will also be synchronized to the server.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code.

**Before you begin**

- Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).
- Configure the XSI host server and the corresponding credentials on the **Voice > Ext (n)** tab.
  - When using **Login Credentials** for XSI server authentication, enter **XSI Host Server**, **Login User ID**, and **Login Password** in the **XSI Line Service** section.
  - When using **SIP Credentials** for XSI server authentication, enter **XSI Host Server** and **Login User ID** in the **XSI Line Service** section, and **Auth ID** and **Password** in the **Subscriber Information** section.
- Disable Feature Key Sync (FKS) in **Call Feature Settings** section from **Voice > Ext (n)**.

**Procedure**

---

**Step 1** Select **Voice > Ext [n]** (where [n] is the extension number).

**Step 2** In the **XSI Line Service** section, set the **CFWD Enable** parameter to **Yes**.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<CFWD_Enable_1_ua="na">Yes</CFWD_Enable_1_>
```

Options: Yes and No

Default: Yes

**Note** If XSI sync for call forward is enabled and the XSI host server or XSI account is not configured correctly, the phone user can't forward calls on the phone.

**Step 3** Click **Submit All Changes**.

**Related Topics**

- [DND and Call Forward Status Sync](#), on page 206
- [Enable Feature Key Sync](#), on page 205

## Enable DND Status Sync via XSI Service

When do not disturb (DND) sync is enabled, the DND setting on the server is synchronized to the phone. The changes in DND setting made on the phone will also be synchronized to the server.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code.

### Before you begin

- Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).
- Configure the XSI host server and the corresponding credentials on the **Voice > Ext (n)** tab.
  - When using **Login Credentials** for XSI server authentication, enter **XSI Host Server**, **Login User ID**, and **Login Password** in the **XSI Line Service** section.
  - When using **SIP Credentials** for XSI server authentication, enter **XSI Host Server** and **Login User ID** in the **XSI Line Service** section, and **Auth ID** and **Password** in the **Subscriber Information** section.
- Disable Feature Key Synchronization (FKS) in **Call Feature Settings** section from **Voice > Ext (n)**.

### Procedure

**Step 1** Select **Voice > Ext [n]** (where [n] is the extension number).

**Step 2** In the **XSI Line Service** section, set the **DND Enable** parameter to **Yes**.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<DND_Enable_1_ ua="na">Yes</DND_Enable_1_>
```

Options: Yes and No

Default: Yes

**Step 3** Click **Submit All Changes**.

### Related Topics

[DND and Call Forward Status Sync](#), on page 206

[Enable Feature Key Sync](#), on page 205

## Enable Synchronization of Anonymous Call Rejection via XSI Service

You can enable synchronization of Anonymous Call Rejection for each line via the XSI service. The function can be used to reject calls from callers who have blocked the display of their number.

Except for the setting for each line, you can also use the **Block ANC Setting** field under the **Supplementary Services** section from **Voice > User** to directly enable or disable the function for all lines.

The priority of the setting: **Block Anonymous Call Enable** > **Block ANC Setting**.

For example, if you set **Block Anonymous Call Enable** to **Yes** for a specific line, the setting in the **Block ANC Setting** doesn't take effect for the line, it takes effect for other lines on which **Block Anonymous Call Enable** is **No**.

### Before you begin

- Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).
- Configure the XSI host server and the corresponding credentials on the **Voice > Ext (n)** tab.
  - When using **Login Credentials** for XSI server authentication, enter **XSI Host Server**, **Login User ID**, and **Login Password** in the **XSI Line Service** section.
  - When using **SIP Credentials** for XSI server authentication, enter **XSI Host Server** and **Login User ID** in the **XSI Line Service** section, and **Auth ID** and **Password** in the **Subscriber Information** section.
- Ensure that Anonymous Call Rejection is enabled on the line or in the XSI service. Otherwise, your user still receives anonymous calls.

### Procedure

---

**Step 1** Select **Voice > Ext [n]** (where [n] is the extension number).

**Step 2** In the **XSI Line Service** section, set the **Block Anonymous Call Enable** parameter to **Yes**.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<Block_Anonymous_Call_Enable_n_ ua="na">Yes</Block_Anonymous_Call_Enable_n_>
```

Where *n* is the extension number.

Options: Yes and No

Default: No

**Step 3** Click **Submit All Changes**.

After the change takes effect, the XSI service takes over the phone to provide the function. The function doesn't work in the following scenarios even though **Block Anonymous Call Enable** is set to **Yes**:

- The function is disabled in the XSI service.
- The function is disabled on the line.

Because the function status is synchronized between the XSI service and the line.

---

## Set Feature Activation Code for Anonymous Call Rejection

You can set activation code to block or remove blocking of anonymous calls for all lines on which synchronization of Anonymous Call Rejection is disabled.

**Before you begin**

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

**Procedure**


---

**Step 1** Select **Voice > Regional**.

**Step 2** In the **Vertical Service Activation Codes** section, ensure that the **Block ANC Act Code** field is set to the value defined by the server. The default value is \*77.

In the phone configuration file with XML(cfg.xml), enter a string in this format:

```
<Block_ANC_Act_Code ua="na">*77</Block_ANC_Act_Code>
```

**Step 3** In the **Vertical Service Activation Codes** section, ensure that the **Block ANC Deact Code** field is set to the value defined by the server. The default value is \*87.

In the phone configuration file with XML(cfg.xml), enter a string in this format:

```
<Block_ANC_Deact_Code ua="na">*87</Block_ANC_Deact_Code>
```

**Step 4** Click **Submit All Changes**.

Your user can dial \*77 or \*87 and press the **Call** softkey to block all anonymous calls or remove the blocking.

This operation is identical to the setting on the **Block ANC Setting** field under the **Supplementary Services** section from **Voice > User**. It takes effect for the lines on which the **Block Anonymous Call Enable** (under the **XSI Line Service** section from **Voice > Ext**) is set to **No**.

---

## Enable Synchronization of Call Waiting via XSI Service

You can enable synchronization of Call Waiting for each line via the XSI service. The function allows the user to receive incoming calls while on another call.

Except for the setting, you can also use the **CW Setting** field under the **Supplementary Services** section from **Voice > User** to directly enable or disable the function for all lines.

The priority of the setting: **Call Waiting Enable > CW Setting**.

For example, if you set **Call Waiting Enable** to **Yes** for a specific line, the setting in the **CW Setting** doesn't take effect for the line, it only takes effect for other lines on which **Call Waiting Enable** is set to **No**.

**Before you begin**

- Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).
- Configure the XSI host server and the corresponding credentials on the **Voice > Ext (n)** tab.
  - When using **Login Credentials** for XSI server authentication, enter **XSI Host Server**, **Login User ID**, and **Login Password** in the **XSI Line Service** section.
  - When using **SIP Credentials** for XSI server authentication, enter **XSI Host Server** and **Login User ID** in the **XSI Line Service** section, and **Auth ID** and **Password** in the **Subscriber Information** section.

- Ensure that Call Waiting is enabled on the line or in the XSI service. Otherwise, your user doesn't receive any incoming calls while on a call.

### Procedure

---

**Step 1** Select **Voice > Ext [n]** (where [n] is the extension number).

**Step 2** In the **XSI Line Service** section, set the **Call Waiting Enable** parameter to **Yes**.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<Call_Waiting_Enable_n_ ua="na">Yes</Call_Waiting_Enable_n_>
```

Where *n* is the extension number.

Options: Yes and No

Default: No

**Step 3** Click **Submit All Changes**.

After the change takes effect, the XSI service takes over the phone to provide the function. The function doesn't work in the following scenarios even though **Call Waiting Enable** is set to **Yes**:

- The function is disabled in the XSI service.
- The function is disabled on the line.

Because the function status is synchronized between the XSI service and the line.

---

## Set Feature Activation Code for Call Waiting

You can set activation code (star code) that can be used to activate or deactivate Call Waiting for all lines.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

---

**Step 1** Select **Voice > Regional**.

**Step 2** In the **Vertical Service Activation Codes** section, ensure that the **CW Act Code** field is set to the value defined by the server. The default value is \*56.

In the phone configuration file with XML(cfg.xml), enter a string in this format:

```
<CW_Act_Code ua="na">*56</CW_Act_Code>
```

**Step 3** In the **Vertical Service Activation Codes** section, ensure that the **CW\_Deact\_Code** field is set to the value defined by the server. The default value is \*57.

In the phone configuration file with XML(cfg.xml), enter a string in this format:

```
<CW_Deact_Code ua="na">*57</CW_Deact_Code>
```

**Step 4** In the **Vertical Service Activation Codes** section, ensure that the **CW\_Per\_Call\_Act\_Code** field is set to the value defined by the server. The default value is \*71.

In the phone configuration file with XML(cfg.xml), enter a string in this format:

```
<CW_Per_Call_Act_Code ua="na">*71</CW_Per_Call_Act_Code>
```

**Step 5** In the **Vertical Service Activation Codes** section, ensure that the **CW\_Per\_Call\_Deact\_Code** field is set to the value defined by the server. The default value is \*70.

In the phone configuration file with XML(cfg.xml), enter a string in this format:

```
<CW_Per_Call_Deact_Code ua="na">*70</CW_Per_Call_Deact_Code>
```

**Step 6** Click **Submit All Changes**.

Your user can dial \*56 or \*57 and press the **Call** softkey to activate or deactivate Call Waiting for all incoming calls. This operation is identical to the setting on the **CW Setting** field under the **Supplementary Services** section from **Voice > User**. These activation codes don't take effect for the lines where synchronization of Call Waiting via the XSI service is enabled.

Your user can dial \*71 or \*70 and press the **Call** softkey to temporarily activate or deactivate Call Waiting for the next incoming call on an active call. These activation codes still take effect for the lines where synchronization of Call Waiting via the XSI service is enabled. If Call Waiting is disabled in the XSI service, the server blocks all incoming calls, therefore these activation codes don't take effect.

## Enable End-of-Call Statistics Reports in SIP Messages

You can enable the phone to send end-of-call statistics in Session Initiation Protocol (SIP) messages (BYE and re-INVITE messages). The phone sends call statistics to the other party of the call when the call terminates or when the call is on hold. The statistics include:

- Real-time Transport Protocol (RTP) packets sent or received
- Total bytes sent or received
- Total number of lost packets
- Delay jitter
- Round-trip delay
- Call duration

The call statistics are sent as headers in SIP BYE messages and SIP BYE response messages (200 OK and re-INVITE during hold). For audio sessions, the headers are **RTP-RxStat** and **RTP-TxStat**.

Example of call statistics in a SIP BYE message:

```
Rtp-Rxstat: Dur=13,Pkt=408,Oct=97680,LatePkt=8,LostPkt=0,AvgJit=0,VQMetrics="CCR=0.0017;ICR=0.0000;ICRmx=0.0077;CS=2;SCS=0;VoRxCodec=PCMU;CID=4;VoPktSizeMs=30;VoPktLost=0;VoPktDis=1;VoOneWayDelayMs=281;maxJitter=12;MOScq=4.21;MOSlq=3.52;network=ethernet;hwType=CP-8865;rtcpBitrate=60110;rtcpBitrate=0"
```

```
Rtp-Txstat: Dur=13,Pkt=417,Oct=100080,tvqMetrics="TxCodec=PCMU;rtptime=61587;rtcpbitrate=0
```

For description of the attributes in call statistics, see [Attributes for Call Statistics in SIP Messages, on page 213](#).

You can also use the `Call_Statistics` parameter in the phone configuration file to enable this feature.

```
<Call_Statistics ua="na">Yes</Call_Statistics>
```

### Before you begin

Access the phone administration web page, see [Access the Phone Web Interface, on page 100](#).

### Procedure

- 
- Step 1** Select **Voice > SIP**.
- Step 2** In the **RTP Parameters** section, set the **Call Statistics** field to **Yes** to enable the phone to send call statistics in SIP BYE and re-INVITE messages.
- You can also configure this parameter in the configuration file (cfg.xml) by entering a string in this format:
- ```
<Call_Statistics ua="na">Yes</Call_Statistics>
```
- The allowed values are Yes|No. The default value is No.
- Step 3** Click **Submit All Changes**.
- 

## Attributes for Call Statistics in SIP Messages

*Table 30: Audio: RTP-RxStat Payload*

Attribute	Description	Mandatory
Dur	Duration of media session/call	Yes
Pkt	Number of RTP packets received	Yes
Oct	Number of RTP packets octets received	No
LatePkt	Number of RTP packets received and discarded as late due to outside of buffer window	Yes
LostPkt	Number of RTP packets lost	Yes
AvgJit	Average Jitter over session duration	Yes
VoRxCCodec	Stream/session codec negotiated	Yes
VoPktSizeMs	Packet size in milliseconds	Yes
maxJitter	Max Jitter detected	Yes
VoOneWayDelayMs	Latency/one way delay	Yes

Attribute	Description	Mandatory
MOScq	Mean opinion score conversational quality for the session, per RFC <a href="https://tools.ietf.org/html/rfc3611">https://tools.ietf.org/html/rfc3611</a>	Yes
maxBurstPktLost	Maximum number of sequential packets lost	No
avgBurstPktLost	Average number of sequential packets lost in a burst. The number can be used in conjunction with overall loss to compare the impact of loss on the call quality.	No
networkType	Type of network the device is on (if possible).	Yes
hwType	Hardware client that the session/media is running on. More relevant for soft clients but still useful for hard phones. For example, Model number CP-8865.	Yes

**Table 31: Audio: RTP-TxStat Payload**

Attribute	Description	Mandatory
Dur	Duration of session	Yes
Pkt	Number of RTP packets transmitted	Yes
Oct	Number of RTP packets octets transmitted	Yes
TxCodec	Transmit codec	Yes
rtpBitRate	Total RTP transmit bit rate (bits/sec)	Yes
rctpBitRate	Total RCTP transmit bit rate (bits/sec)	Yes

## SIP Session ID

The Multiplatform phones now support “Session Identifier”. This feature helps to overcome the limitations with the existing call-identifiers and allows end-to-end tracking of a SIP session in IP-based multimedia communication systems in compliance with RFC 7989. To support session identifier, “Session-ID” header is added in the SIP request and response messages.

"Session Identifier" refers to the value of the identifier, whereas "Session-ID" refers to the header field used to convey the identifier.

- When a user initiates the call, the phone while sending SIP INVITE message, generates the local-UUID.
- When the UAS receives the SIP-INVITE, the phone picks up the local UUIDs with the incoming messages and appends it to the received Session-ID header and sends the header in responses.
- The same UUIDs are maintained in all the SIP messages of a particular session.
- The phone maintains the same local-UUID during other features, such as conference or transfer.
- This header is implemented in REGISTER method, the local-UUID remains same for all the REGISTER messages till the phone fails to REGISTER.



The Session-ID comprises of Universally Unique Identifier (UUID) for each user agent participating in a call. Each call consists of two UUID known as local UUID and remote UUID. Local UUID is the UUID generated from the originating user agent and remote UUID is generated from the terminating user agent. The UUID values are presented as strings of lower-case hexadecimal characters, with the most significant octet of the UUID appearing first. Session Identifier comprises of 32 characters and remains same for the entire session.

### Session ID format

Components will implement Session-ID which is global session ID ready.

A sample current session ID passed in http header by phones (dashes are just included for clarity) is 00000000-0000-0000-0000-5ca48a65079a.

A session-ID format: UUUUUUUUSSSS5000y00DDDDDDDDDDDDDD where,

UUUUUUUU - A randomly generated unique ID[0-9a-f] for the session. Examples of new session IDs generated are:

- Phone going off hook
- Entry of the activation code through to first SIP first registration (the onboarding flow)

SSSS - The source that generates the session. For example, if the source type is "Cisco MPP" the source value (SSSS) can be "0100".

Y - Any of the values of 8, 9, A, or B and should be compliant with UUID v5 RFC.

DDDDDDDDDDDD - MAC address of the phone.

### SessionID Example in SIP Messages

This header is supported in the in-call dialog messages like INVITE/ACK/CANCEL/BYE/UPDATE/INFO/REFER and their responses as well as out-of-call messages essentially the REGISTER.

```
Request-Line: INVITE sip:901@10.89.107.37:5060 SIP/2.0
      Session-ID: 298da61300105000a00000ebd5cbd5c1;remote=00000000000000000000000000000000

Status-Line: SIP/2.0 100 Trying
      Session-ID: fbbaa810a00105000a00000ebd5cc118b;remote=298da61300105000a00000ebd5cbd5c1

Status-Line: SIP/2.0 180 Ringing
      Session-ID: fbbaa810a00105000a00000ebd5cc118b;remote=298da61300105000a00000ebd5cbd5c1

Status-Line: SIP/2.0 200 OK
      Session-ID: fbbaa810a00105000a00000ebd5cc118b;remote=298da61300105000a00000ebd5cbd5c1

Request-Line: ACK sip:901@10.89.107.37:5060 SIP/2.0
      Session-ID: 298da61300105000a00000ebd5cbd5c1;remote=fbbaa810a00105000a00000ebd5cc118b

Request-Line: BYE sip:901@10.89.107.37:5060 SIP/2.0
      Session-ID: 298da61300105000a00000ebd5cbd5c1;remote=fbbaa810a00105000a00000ebd5cc118b

Status-Line: SIP/2.0 200 OK
      Session-ID: fbbaa810a00105000a00000ebd5cc118b;remote=298da61300105000a00000ebd5cbd5c1
```

## Enable SIP Session ID

You can enable SIP session ID to overcome the limitations with the existing call-identifiers and to allow end-to-end tracking of a SIP session.

**Before you begin**

[Access the Phone Web Interface, on page 100](#)

**Procedure**

- 
- Step 1** Select **Voice > Ext(n)**.
- Step 2** Go to the **SIP Settings** section.
- Step 3** Set the **SIP SessionID Support** field as described in the [Session ID Parameters, on page 216](#) table.
- Step 4** Click **Submit All Changes**.
- 

## Session ID Parameters

The following table defines the function and usage of each parameter in the **SIP Settings** section in the **Voice > Ext(n)** tab of the phone web page. It also defines the syntax of the string that is added in the phone configuration file with XML (cfg.xml) code to configure a parameter.

Parameter Name	Description and Default Value
SIP SessioID Support	<p>Controls the SIP session ID support.</p> <p>Perform one of the following</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML (cfg.xml) enter a string in this format.           <pre>&lt;SIP_SessionID_Support_1_ua="na"&gt;Yes&lt;/SIP_SessionID_Support_1_&gt;</pre> </li> <li>In the phone web page select <b>Yes</b> to enable the feature.</li> </ul> <p>Allowed values: Yes/No</p> <p>Default: Yes.</p>

## Set Up a Phone for Remote SDK

You can configure remote SDK for a multiplatform phone. The remote SDK provides a WebSocket based protocol through which the phone can be controlled.

**Before you begin**

- [Access the Phone Web Interface, on page 100](#)
- A WebSocket server must be running with an address and port reachable from the phone.

## Procedure

- 
- Step 1** Select **Voice > Phone**.
- Step 2** Go to the **WebSocket API** section.
- Step 3** Set the **Control Server URL** and the **Allowed APIs** fields as described in the [WebSocket API Parameters, on page 217](#) table.
- Step 4** Click **Submit All Changes**.
- 

## WebSocket API Parameters

The following table defines the function and usage of each parameter in the **WebSocket API** section in the **Voice > Phone** tab of the phone web page. It also defines the syntax of the string that is added in the phone configuration file with XML (cfg.xml) code to configure a parameter.

Parameter Name	Description and Default Value
Control Server URL	<p>The URL of a WebSocket server to which the phone attempts to stay connected.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML (cfg.xml) enter a string in this format.</li> </ul> <pre>&lt;Control_Server_URL ua="na"/&gt;</pre> <ul style="list-style-type: none"> <li>In the phone web page enter the URL of a WebSocket server.</li> </ul> <p>For example:</p> <pre>&lt;Control_Server_URL&gt;wss://my-server.com/ws-server-path&lt;/Control_Server_URL&gt;</pre> <p>The URL should be in one of the following formats:</p> <ul style="list-style-type: none"> <li>For a nonsecure HTTP connection: <b>ws://your-server-name/path</b></li> <li>For a secure HTTPS connection: <b>wss://your-server-name/some-path</b></li> </ul> <p>We recommend a secure connection.</p> <p>Default: Empty.</p>

Parameter Name	Description and Default Value
Allowed APIs	<p>A regular expression that can be used to limit the API calls that are allowed from the controlling server.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml) enter a string in this format.  <pre>&lt;Allowed_APIS ua="na"&gt;.*&lt;/Allowed_APIS&gt;</pre> </li> <li>In the phone web page enter an appropriate regular expression.</li> </ul> <p>The regular expression provided is matched with the Request-URI path provided in the API request from the controlling server. If the entire path is not matched by the given regular expression, the API call is rejected.</p> <p>Allowed values are:</p> <ul style="list-style-type: none"> <li>.*: All APIs are allowed</li> <li>/api/Call/v1/.*: All v1 <b>Call</b> interface calls are allowed.</li> <li>/api/Call/v1/(Dial Hangup): Only the v1 Call interface calls <b>Dial</b> and <b>Hangup</b> are allowed.</li> </ul> <p>Default: .*</p>

## Hide a Menu Item from Being Displayed on the Phone Screen

By default, all the menu items on the phone screen **Information and settings** are visible to users. You can configure the phone to hide or show specific menu items. When hidden, the items don't display on the phone screen.

You can hide any of the following menu items as needed:

- Speed dials
- User preferences
- Network configuration
- Device administration
- Status
- Report problem

You can also configure the visibility of the menu items in the configuration file (cfg.xml) with strings in this format:

```
<Device_Administration ua="na">No</Device_Administration>
```

See the parameter syntax and valid values in [Parameters for Menu Visibility, on page 219](#).

## Procedure

- 
- Step 1** Select **Voice > Phone**.
- Step 2** In the **Menu Visibility** section, set the menu items that you want to hide to **No**.
- Step 3** Click **Submit All Changes**.
- 

## Parameters for Menu Visibility

The following table defines the function and usage of each parameter in the **Menu Visibility** section of the **Voice > Phone** tab.

*Table 32: Parameters for Menu Visibility*

Parameter Name	Description and Default Value
Speed Dials	<p>Controls whether to show the <b>Speed dials</b> menu on the phone screen. Set this field to <b>Yes</b> to show the menu. Otherwise, set it to <b>No</b>.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file (cfg.xml) with XML, enter a string in this format:           <pre>&lt;Speed_Dials ua="na"&gt;Yes&lt;/Speed_Dials&gt;</pre> </li> <li>In the phone web interface, select <b>Yes</b> or <b>No</b> to show or hide the menu.</li> </ul> <p>Valid values: Yes and No</p> <p>Default: Yes</p>
User Preferences	<p>Controls whether to show the <b>User preferences</b> menu on the phone screen. Set this field to <b>Yes</b> to show the menu. Otherwise, set it to <b>No</b>.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file (cfg.xml) with XML, enter a string in this format:           <pre>&lt;User_Preferences ua="na"&gt;Yes&lt;/User_Preferences&gt;</pre> </li> <li>In the phone web interface, select <b>Yes</b> or <b>No</b> to show or hide the menu.</li> </ul> <p>Valid values: Yes and No</p> <p>Default: Yes</p>

Parameter Name	Description and Default Value
Network Configuration	<p>Controls whether to show the <b>Network configuration</b> menu on the phone screen. Set this field to <b>Yes</b> to show the menu. Otherwise, set it to <b>No</b>.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file (cfg.xml) with XML, enter a string in this format:  <pre>&lt;Network_Configuration ua="na"&gt;Yes&lt;/Network_Configuration&gt;</pre> </li> <li>In the phone web interface, select <b>Yes</b> or <b>No</b> to show or hide the menu.</li> </ul> <p>Valid values: Yes and No Default: Yes</p>
Device Administration	<p>Controls whether to show the <b>Device administration</b> menu on the phone screen. Set this field to <b>Yes</b> to show the menu. Otherwise, set it to <b>No</b>.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file (cfg.xml) with XML, enter a string in this format:  <pre>&lt;Device_Administration ua="na"&gt;Yes&lt;/Device_Administration&gt;</pre> </li> <li>In the phone web interface, select <b>Yes</b> or <b>No</b> to show or hide the menu.</li> </ul> <p>Valid values: Yes and No Default: Yes</p>
Status	<p>Controls whether to show the <b>Status</b> menu on the phone screen. Set this field to <b>Yes</b> to show the menu. Otherwise, set it to <b>No</b>.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file (cfg.xml) with XML, enter a string in this format:  <pre>&lt;Status ua="na"&gt;Yes&lt;/Status&gt;</pre> </li> <li>In the phone web interface, select <b>Yes</b> or <b>No</b> to show or hide the menu.</li> </ul> <p>Valid values: Yes and No Default: Yes</p>

Parameter Name	Description and Default Value
Report Problem	<p>Controls whether to show the <b>Report problem</b> menu under the <b>Status</b> menu on the phone screen. Set this field to <b>Yes</b> to show the menu. Otherwise, set it to <b>No</b>.</p> <p>When the <b>Status</b> menu is invisible, the <b>Report problem</b> menu is invisible as well.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file (cfg.xml) with XML, enter a string in this format: <pre>&lt;Report_Problem_Menu ua="na"&gt;Yes&lt;/Report_Problem_Menu&gt;</pre> </li> <li>In the phone web interface, select <b>Yes</b> or <b>No</b> to show or hide the menu.</li> </ul> <p>Valid values: Yes and No</p> <p>Default: Yes</p>

## Display Caller Number Instead of Unresolved Caller Name

By default, the phone displays both the caller name and the caller number in an incoming call alert. When the phone can't resolve the characters in caller name, the user sees boxes instead of the caller name. You can configure the phone to display only the number when any unresolved characters are detected in the caller name.

### Procedure

**Step 1** Select **Voice > Regional**.

**Step 2** In the **Language** section, set the **Replace Unresolved Caller Name with Number** field to **Yes**.

You can also configure this parameter in the configuration file (cfg.xml) with a string in this format:

```
<Replace_Unresolved_Caller_Name_with_Number
ua="na">Yes</Replace_Unresolved_Caller_Name_with_Number>
```

The valid values are Yes and No. The default setting is No.

**Step 3** Click **Submit All Changes**.

# Menu Shortcuts Mapping on PSK

Table 33: Menu Shortcuts Mapping

Function (fnc=)	URL String (url=)	Target Menu
shortcut	settings	<b>Settings</b>
shortcut	accessibility	<b>Settings &gt; Accessibility</b>
shortcut	recents	<b>Settings &gt; Recents</b>
shortcut	allcalls	<b>Settings &gt; Recents &gt; All calls</b>
shortcut	missedcalls	<b>Settings &gt; Recents &gt; Missed calls</b>
shortcut	receivedcalls	<b>Settings &gt; Recents &gt; Received calls</b>
shortcut	placedcalls	<b>Settings &gt; Recents &gt; Placed calls</b>
shortcut	speeddials	<b>Settings &gt; Speed dials</b>
shortcut	userpref	<b>Settings &gt; User preferences</b>
shortcut	callpref	<b>Settings &gt; User preferences &gt; Call preferences</b>
shortcut	cfwsetting	<b>Settings &gt; User preferences &gt; Call preferences &gt; Call forwarding</b>
shortcut	anywhere	<b>Settings &gt; User preferences &gt; Call preferences &gt; Anywhere</b>
shortcut	audiopref	<b>Settings &gt; User preferences &gt; Audio preferences</b>
shortcut	screenpref	<b>Settings &gt; User preferences &gt; Screen preferences</b>
shortcut	screensaver	<b>Settings &gt; User preferences &gt; Screen preferences &gt; Screen saver</b>
shortcut	attconsole	<b>Settings &gt; User preferences &gt; Attendant console preferences</b>
shortcut	ringtone	<b>Settings &gt; User preferences &gt; Ringtone</b>
shortcut	bluetooth	<b>Settings &gt; Bluetooth</b>
shortcut	networkconf	<b>Settings &gt; Network configuration</b>
shortcut	ethernetconf	<b>Settings &gt; Network configuration &gt; Ethernet configuration</b>
shortcut	ipv4setting	<b>Settings &gt; Network configuration &gt; IPv4 address settings</b>
shortcut	ipv6setting	<b>Settings &gt; Network configuration &gt; IPv6 address settings</b>
shortcut	adminsetting	<b>Settings &gt; Device administration</b>



<b>Function (fnc=)</b>	<b>URL String (url=)</b>	<b>Target Menu</b>
shortcut	setpassword	<b>Settings &gt; Device administration &gt; Set password</b>
shortcut	usersignin	<b>Settings &gt; Device administration &gt; Sign in</b>
shortcut	usersignout	<b>Settings &gt; Device administration &gt; Sign out</b>
shortcut	datetime	<b>Settings &gt; Device administration &gt; Date/Time</b>
shortcut	language	<b>Settings &gt; Device administration &gt; Language</b>
shortcut	restart	<b>Settings &gt; Device administration &gt; Restart</b>
shortcut	factoryreset	<b>Settings &gt; Device administration &gt; Factory reset</b>
shortcut	profilerule	<b>Settings &gt; Device administration &gt; Profile rule</b>
shortcut	profileaccount	<b>Settings &gt; Device administration &gt; Profile account setup</b>
shortcut	microphones	<b>Settings &gt; Device administration &gt; Microphones</b>
shortcut	wiredmic	<b>Settings &gt; Device administration &gt; Microphones &gt; Wired microphones</b>
shortcut	wirelessmic	<b>Settings &gt; Device administration &gt; Microphones &gt; Wireless microphones</b>
shortcut	status	<b>Settings &gt; Status</b>
shortcut	productinfo	<b>Settings &gt; Status &gt; Product information</b>
shortcut	networkstatus	<b>Settings &gt; Status &gt; Network status</b>
shortcut	ipv4status	<b>Settings &gt; Status &gt; Network status &gt; IPv4 status</b>
shortcut	ipv6status	<b>Settings &gt; Status &gt; Network status &gt; IPv6 status</b>
shortcut	phonestatus	<b>Settings &gt; Status &gt; Phone status</b>
shortcut	phonestat	<b>Settings &gt; Status &gt; Phone status &gt; Phone status</b>
shortcut	linestatus	<b>Settings &gt; Status &gt; Phone status &gt; Line status</b>
shortcut	provstatus	<b>Settings &gt; Status &gt; Phone status &gt; Provisioning</b>
shortcut	callstat	<b>Settings &gt; Status &gt; Phone status &gt; Call statistics</b>
shortcut	reportproblem	<b>Settings &gt; Status &gt; Report problem</b>
shortcut	reboothistory	<b>Settings &gt; Status &gt; Reboot history</b>
shortcut	accessories	<b>Settings &gt; Status &gt; Accessories</b>
shortcut	statusmessage	<b>Settings &gt; Status &gt; Status messages</b>

<b>Function (fnc=)</b>	<b>URL String (url=)</b>	<b>Target Menu</b>
shortcut	directories	<b>Directories</b>
shortcut	personaldir	<b>Directories &gt; Personal address book</b>
shortcut	alldir	<b>Directories &gt; All</b>
shortcut	ldapdir	<b>Directories &gt; Corporate directory (LDAP)</b> The LDAP directory name is customizable.
shortcut	broadsoftdir	<b>Directories &gt; BroadSoft directory</b> The BroadSoft directory name is customizable.
shortcut	bsdirpers	<b>Directories &gt; BroadSoft directory &gt; Personal</b> The BroadSoft directory name is customizable.
shortcut	bsdirgrp	<b>Directories &gt; BroadSoft directory &gt; Group</b> The BroadSoft directory name is customizable.
shortcut	bsdirent	<b>Directories &gt; BroadSoft directory &gt; Enterprise</b> The BroadSoft directory name is customizable.
shortcut	bsdirgrpcom	<b>Directories &gt; BroadSoft directory &gt; Group common</b> The BroadSoft directory name is customizable.
shortcut	bsdirentcom	<b>Directories &gt; BroadSoft directory &gt; Enterprise common</b> The BroadSoft directory name is customizable.
shortcut	xmppdir	<b>Directories &gt; IM&amp;P contacts</b> The XMPP directory name is customizable.
shortcut	xmlapp	<b>Settings &gt; Cisco XML services</b> The XML application name is customizable.
shortcut	xmldir	<b>Directories &gt; Corporate directory (XML)</b> The XML directory name is customizable.
shortcut	webexdir	<b>Directories &gt; Webex directory</b> The Webex directory name is customizable. By default, the softkey displays the directory name as <b>Webex Dir.</b>
shortcut	proxysset	<b>Settings &gt; Network configuration &gt; HTTP proxy settings</b>

# Add a Menu Shortcut to a Programmable Softkey

You can configure a softkey as a phone menu shortcut.

## Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

## Procedure

---

**Step 1** Select **Voice > Phone**.

**Step 2** In the **Programmable Softkeys** section, set the **Programmable Softkey Enable** field to **Yes**.

You can also configure the parameter in the configuration file (cfg.xml) with a string in this format:

```
<Programmable_Softkey_Enable ua="rw">Yes</Programmable_Softkey_Enable>
```

**Step 3** Configure a PSK field from PSK 1 through PSK 16 with a string in this format:

```
fnc=shortcut;url=userpref;nme=User preferences
```

where:

- fnc= shortcut means function=phone menu shortcut.
- url= userpref is the menu to open with this line key. It's the **User preferences** menu in this example. For more shortcut mapping, see [Menu Shortcuts Mapping on PSK, on page 222](#).
- nme= XXXX is the menu shortcut name displayed on the phone. In the example, the softkey displays **User preferences**.

You can also configure this parameter in the configuration file (cfg.xml). Enter a string in this format:

```
<PSK_n ua="rw">fnc=shortcut;url=userpref;nme=User preferences</PSK_n>
```

where *n* is the PSK number.

**Step 4** Add the configured PSK to the desired key list.

**Example:** Add the configured **PSK 2** to **Idle Key List**. Do any of these actions:

- Add `psk2` to the **Idle Key List** field.

```
psk2;em_login;acd_login;acd_logout;astate;redial;cfwd;dnd;lcr;
```

- In the configuration file (cfg.xml), enter a string in this format:

```
<Idle_Key_List  
ua="rw">psk2;em_login;acd_login;acd_logout;astate;redial;cfwd;dnd;lcr;</Idle_Key_List>
```

**Step 5** Click **Submit All Changes**.

---

# Enable LDAP Unified Search

You can enable the unified search in the LDAP directory. The search allows you to enter any value as filters. For example, first name, last name, extension, or phone number. The phone transfers the request as a single search request.

## Before you begin

- Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).
- **Browse Mode Enable** parameter set to **Yes** or **No**.

## Procedure

---

**Step 1** Select **Voice > Phone**.

**Step 2** In the **LDAP** section, set the parameter **Unified Search Enable** to **Yes** to enable the LDAP unified search. If the parameter is set to **Yes**, the phone transfers requests with OR filter.

If you set the value to **No**, the phone uses simple or advanced search and transfers requests with AND filter.

Default value is **No**.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<LDAP_Unified_Search_Enable>Yes</LDAP_Unified_Search_Enable>
```

Conditions based on **Browse Mode Enable** and **Unified Search Enable** parameter values:

- **Browse Mode Enable** parameter is **No** and **Unified Search Enable** parameter is **No** - when the user chooses the LDAP directory on the phone, the **Query LDAP server** screen displays **Simple search** and **Advanced search** menus.
- **Browse Mode Enable** parameter is **No** and **Unified Search Enable** parameter is **Yes** - when the user chooses the LDAP directory, the phone navigates to the **LDAP query form** (unified search screen) directly. If there is no value in the search box, the search displays all contacts in the directory.
- **Browse Mode Enable** parameter is **Yes** and **Unified Search Enable** parameter is **No** - when the user navigates to the LDAP directory and clicks the **Option** softkey, the phone displays the **Simple search** and the **Advanced search** menus.
- **Browse Mode Enable** parameter is **Yes** and **Unified Search Enable** parameter is **Yes** - when the user navigates to the LDAP directory and clicks the **Option** softkey, the phone displays only one **Search** menu. After clicking the **Search** menu, the unified search screen **LDAP query form** appears.

**Step 3** Click **Submit All Changes**.

---



## CHAPTER 11

# Phone Information and Display Configuration

---

- [Phone Information and Display Settings, on page 227](#)
- [Configure the Phone Name, on page 227](#)
- [Customize the Startup Screen, on page 228](#)
- [Customize Wallpaper for the Phone Display, on page 229](#)
- [Configure the Screen Saver with the Phone Web Interface, on page 230](#)
- [Adjust Backlight Timer from the Phone Web Interface, on page 233](#)
- [Customize the Product Configuration Version, on page 234](#)
- [Keep Focus on the Active Call, on page 234](#)

## Phone Information and Display Settings

The phone web user interface allows you to customize settings such as the phone name, background picture, logo, and screen saver.

## Configure the Phone Name

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

---

**Step 1** Select **Voice > Phone**.

**Step 2** Under **General**, enter the phone name in the **Station Display Name** field.

This name displays on the phone screen. You can also configure this parameter in the configuration file (cfg.xml) by entering a string in this format:

```
<Station_Display_Name ua="na">Recetion Desk</Station_Display_Name>
```

**Step 3** Click **Submit All Changes**.

---

# Customize the Startup Screen

You can create a text or an image logo to display when the Cisco IP Phone boots up. A logo displays during the boot sequence for a short period after the Cisco logo displays.

## Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

## Procedure

**Step 1** Click **Voice > User**.

**Step 2** In the **Screen** section, select any option from the **Boot Display** field.

- **Default:** Displays a blank screen or existing screen as the startup screen.
- **Download Picture:** Displays a picture as the startup screen. Enter the path in the **Picture Download URL** field.
- **Logo:** Displays a logo as the startup screen. Enter the path in the **Logo URL** field.
- **Text:** Displays a text as the startup screen. Enter text in the **Text Display** field.

You can also configure this parameter in the configuration file (cfg.xml) by entering a string in this format:

```
<Boot_Display ua="na">Logo</Boot_Display>
```

The allowed values are Default|Download Picture|Logo|Text. The default option is Default.

**Step 3** To display a picture or a logo, enter the path in the **Picture Download URL** or **Logo URL** field.

For example:

```
http://10.64.84.147/pictures/image04.png
```

When you enter an incorrect URL to download the image, the phone fails to upgrade to the new image and displays the existing image. If the phone does not have any image downloaded earlier, it displays a gray screen.

The logo must be a .jpg or a .png file. The phone has a fixed display area. So, if the original logo size doesn't fit into the display area, you need to scale it to fit the screen. The display area size of the Cisco IP Phone 8832 is 48x48.

You can also configure this parameter in the configuration file (cfg.xml) by entering a string in this format:

```
<Picture_Download_URL
ua="na">http://10.64.84.147/pictures/bootimage1.jpg</Picture_Download_URL>
<Logo_URL ua="na">http://10.64.84.147/pictures/logo_image.jpg</Logo_URL>
```

**Step 4** To display text at bootup, enter the text to display in the **Text Display** field following the requirements:

- Enter up to two lines of text with less than 32 characters for each line.
- Insert a new line character (\n) and escape code (%0a) between the two lines.

For example,

```
Super\n%0aTelecom
```

displays:

```
 Super
Telecom
```

- Use the + character to add spaces for formatting. You can add multiple + characters before and after the text to center it.

You can also configure this parameter in the configuration file (cfg.xml) by entering a string in this format:

```
<Text_Display ua="na">Super\n%0aTelecom</Text_Display>
```

**Step 5** Click **Submit All Changes**.

The phone reboots, retrieves the image file, and displays the picture, logo, or text when it boots next time.

---

## Customize Wallpaper for the Phone Display

You can set the phone to display a custom logo or picture as the background on the phone screen.

### Procedure

---

**Step 1** On the phone web interface, select **Voice > User**.

User can also change the wallpaper in the phone web interface.

**Step 2** In the **Screen** section, choose one of the options for the **Phone Background** field:

- **Default**—Keeps the system default background.
- **Download Picture**—Displays a picture downloaded from a TFTP, FTP, or HTTPS server. When select this option, enter the URL for the picture in the **Picture Download URL** field.
- **Logo**—Displays a logo downloaded from a TFTP, FTP, or HTTPS server. When select this option, enter the URL for the logo image in the **Logo URL** field.

You can also configure this parameter in the configuration file (cfg.xml) by entering a string in this format:

```
<Phone_Background ua="na">Logo</Phone_Background>
```

**Step 3** Upload the custom wallpaper to a TFTP, HTTP, or HTTPS server.

The image is a .jpg or .png file. Preferred dimension is 480x128 pixels. If the image is not the preferred size, user still can upload it but it will resize to fit the screen.

**Step 4** In the **Picture Download URL** field, enter the path where the wallpaper image has been uploaded.

The URL must include the TFTP, HTTP, or HTTPS server name (or IP address), directory, and file name. Don't exceed 255 characters for the URL.

Example:

```
http://10.64.84.147/pictures/image04.jpg
```

When you enter an incorrect URL to download a new wallpaper, the phone fails to upgrade to the new wallpaper and displays the existing downloaded wallpaper. If the phone does not have any wallpaper downloaded earlier, it displays a gray screen.

You can also configure this parameter in the configuration file (cfg.xml) by entering a string in this format:

```
<Picture_Download_URL ua="na">http://10.64.84.147/pictures/image04.jpg</Picture_Download_URL>
```

**Step 5** Upload the logo image to a TFTP, HTTP, or HTTPS server.

The logo must be a .jpg or a .png file. The phone has a fixed display area. So, if the original logo size doesn't fit into the display area, you need to scale it to fit the screen. The display area size of the Cisco IP Phone 8832 is 48x48.

**Step 6** In the **Logo URL** field, enter the path where the logo image has been uploaded.

The URL must include the TFTP, HTTP, or HTTPS server name (or IP address), directory, and file name. Don't exceed 255 characters for the URL.

Example:

```
http://10.64.84.147/pictures/logo_image.jpg
```

When you enter an incorrect URL to download a new logo, the phone fails to upgrade to the newer logo and displays the existing downloaded logo. If the phone does not have any logo downloaded earlier, it displays a gray screen.

You can also configure this parameter in the configuration file (cfg.xml) by entering a string in this format:

```
<Logo_URL ua="na">http://10.64.84.147/pictures/logo_image.jpg</Logo_URL>
```

**Step 7** Click **Submit All Changes**.

The phone reboots after you change the background image URL.

## Configure the Screen Saver with the Phone Web Interface

You can configure a screen saver for the phone. When the phone is idle for a specified time, it enters screen saver mode.

Any button press returns the phone to normal mode.

You can also configure the parameters in the phone configuration file with XML (cfg.xml) code. To configure each parameter, see the syntax of the string in [Parameters for Screen Saver, on page 231](#).

### Before you begin

Access the phone administration web interface. See [Access the Phone Web Interface, on page 100](#).

### Procedure

**Step 1** On the phone web page, select **Voice > User**.

The user can select **User Login > Voice > User** to add screen saver to the phone.



- Step 2** In the **Screen** section, set up the fields as described in [Parameters for Screen Saver, on page 231](#).
- Step 3** Click **Submit All Changes**.

## Parameters for Screen Saver

The following table defines the function and usage of the screen saver parameters in the **Screen** section under the **Voice> User** tab in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file (cfg.xml) with XML code to configure a parameter.

**Table 34: Parameters for Screen Saver**

Parameter	Description
Screen Saver Enable	<p>Select <b>Yes</b> to enable a screen saver on the phone. When the phone is idle for a specified time, it enters screen saver mode.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:           <pre data-bbox="1015 940 1437 989">&lt;Screen_Saver_Enable ua="rw"&gt;Yes&lt;/Screen_Saver_Enable&gt;</pre> </li> <li>In the phone web interface, set this field to <b>Yes</b> to enable screen saver.</li> </ul> <p>Allowed values: Yes No</p> <p>Default: No</p>

Parameter	Description
Screen Saver Type	<p>Types of screen saver. Options you can choose:</p> <ul style="list-style-type: none"> <li>• <b>Clock</b>—Displays a digital clock on a plain background.</li> <li>• <b>Download Picture</b>—Displays a picture pushed from the phone webpage. Enter the image path in the <b>Picture Download URL</b> field.</li> <li>• <b>Logo</b>: Displays a logo on the phone screen. Add a logo image in the <b>Logo URL</b> field.</li> </ul> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>• In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="976 758 1398 810">&lt;Screen_Saver_Type ua="rw"&gt;Clock&lt;/Screen_Saver_Type&gt;</pre> </li> <li>• In the phone web interface, select a screen saver.</li> </ul> <p>Allowed values: Clock Download Picture Logo Default: Clock</p>
Screen Saver Wait	<p>Amount of idle time before screen saver displays. Enter the number of seconds of idle time to elapse before the screen saver starts.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>• In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="976 1255 1373 1308">&lt;Screen_Saver_Wait ua="rw"&gt;300&lt;/Screen_Saver_Wait&gt;</pre> </li> <li>• In the phone web interface, set the time in seconds.</li> </ul> <p>Allowed values: An integer from 30 through 65000 Default: 300</p>

Parameter	Description
Picture Download URL	<p>URL locating the (.png) file to display on the phone screen background. The image can display as the screen background, the screensaver, or at bootup depending on the settings of the <b>Phone Background</b>, <b>Screen Saver Type</b>, or <b>Boot Display</b> field.</p> <p>When you enter an incorrect URL to download a new image, the phone fails to update to the new image and displays the existing downloaded image. If the phone does not have any image downloaded earlier, it displays a gray screen.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="1015 772 1528 821">&lt;Picture_Download_URL ua="rw"&gt;http://10.74.3.52/images/screensaver1.png&lt;/Picture_Download_URL&gt;</pre> </li> <li>In the phone web interface, specify the URL where the picture is located.</li> </ul> <p>Allowed values: A valid URL not exceeding 255 characters</p> <p>Default: Empty</p>
Logo URL	<p>Enter a URL or path for the location where the logo image is saved. The logo image can display as the screen background, the screensaver, or at bootup depending on the settings of the <b>Screen Saver Type</b>, <b>Boot Display</b>, or <b>Phone Background</b> field.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="1015 1377 1528 1425">&lt;Logo_URL ua="rw"&gt;http://10.74.3.52/images/Logo1.png&lt;/Logo_URL&gt;</pre> </li> <li>In the phone web interface, specify the URL where the logo image is located.</li> </ul> <p>Allowed values: A valid URL not exceeding 255 characters</p> <p>Default: Empty</p>

## Adjust Backlight Timer from the Phone Web Interface

You can save energy by disabling the backlight on each phone at a preset time.

### Procedure

---

- Step 1** Select **Voice > User**.
- Step 2** In the **Screen** section, select a duration for the **Back Light Timer** parameter.
- You can also configure this parameter in the configuration file (cfg.xml) by entering a string in this format:
- ```
<Back_Light_Timer ua="rw">30s</Back_Light_Timer>
```
- Step 3** Click **Submit All Changes**.
- 

## Customize the Product Configuration Version

You can customize the configuration version of the product in the phone configuration file (cfg.xml). After the change takes effect, the user can view the configuration version of the product information on the phone.

### Procedure

---

- Step 1** Edit the phone configuration file (cfg.xml) in a text or XML editor.
- Step 2** Add a value for the element `<Device_Config_Version>` in the cfg.xml file.
- For example:
- ```
<Device_Config_Version ua="na">2021-01-05-v1</Device_Config_Version>
```
- Default: Empty
- Value range: 0 to 64 characters
- If the tag doesn't exist in the cfg.xml file or the parameter value is empty, then the **Configuration version** menu item doesn't display on the phone screen **Product information**.
- Step 3** Save the changes to the cfg.xml file.
- 

## Keep Focus on the Active Call

You can configure the phone to ensure that the active call is still in focus when the user has an incoming call.

By default, the focus on the phone screen automatically moves from the active call to the incoming call. However, you can configure the phone to ensure that the active call always remains in focus, even when the user has an incoming call.

The focus still moves to an incoming call in the following situations:

- The user places an active call on hold and then receives one or more incoming calls, the focus automatically moves to the first incoming call.
- The user is on an active call and receives one or more incoming calls, if the user places the active call on hold, then the focus automatically moves to the first incoming call.

**Before you begin**

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

**Procedure**

---

- Step 1** Select **Voice > User**.
- Step 2** In the **Supplementary Services** section, set the parameter **Keep Focus On Active Call** to **Yes**.  
You can also configure this parameter in the configuration file:  

```
<Keep_Focus_On_Active_Call ua="na">Yes</Keep_Focus_On_Active_Call>
```

  
Allowed values: Yes and No  
Default: No
- Step 3** Click **Submit All Changes**.
-

Keep Focus on the Active Call



## CHAPTER 12

# Call Features Configuration

The phone web user interface and the xml configuration files allows you to customize calling features of your phone such as call transfer, call park, conferencing, and speed-dial.

- [Enable Call Transfer, on page 237](#)
- [Call Forward, on page 239](#)
- [Enable Feature Activation Code Synchronization for Forward All Calls, on page 245](#)
- [Enable Conferencing, on page 247](#)
- [Enable Remote Call Recording with SIP REC, on page 247](#)
- [Enable Remote Call Recording with SIP INFO, on page 249](#)
- [Configure Missed Call Indication , on page 250](#)
- [Enable Do Not Disturb, on page 250](#)
- [Enable Synchronization of Settings Between the Phone and the Server, on page 251](#)
- [Enable Webex Contacts on the Phone, on page 252](#)
- [Configure Webex Contacts on a Line Key, on page 253](#)
- [Add a Softkey for Webex Contacts, on page 254](#)
- [Enable Webex Call Logs on the Phone, on page 255](#)
- [Configure Star Codes for DND, on page 255](#)
- [Set Up a Call Center Agent Phone, on page 256](#)
- [Set Up a Phone for Presence, on page 261](#)
- [Configure the Number of Call Appearances Per Line, on page 264](#)
- [Enable Reverse Name Lookup, on page 264](#)
- [Emergency Calls, on page 266](#)
- [Spam Indication for Incoming Webex Calls, on page 270](#)
- [Programmable Softkeys Configuration, on page 271](#)

## Enable Call Transfer

You can enable attended call transfer and blind call transfer services for your user.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code. To configure each parameter, see the syntax of the string in [Parameters for Enable Call Transfer, on page 238](#) table.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

## Procedure

- 
- Step 1** Select **Voice > Phone**.
- Step 2** Under **Supplementary Services**, configure the parameters as defined in the [Parameters for Enable Call Transfer](#), on page 238 table.
- Step 3** Click **Submit All Changes**.
- 

## Parameters for Enable Call Transfer

The following table defines the function and usage of Enable Call Transfer parameters in the Supplementary Services section under the Phone tab in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file with XML(cfg.xml) code to configure a parameter.

*Table 35: Parameters for Enable Call Transfer*

Parameter	Description
Attn Transfer Serv	<p>Attended call transfer service. The user answers the call before transferring it.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;Attn_Transfer_Serv ua="na"&gt;Yes&lt;/Attn_Transfer_Serv&gt;</pre> </li> <li>In the phone web page, select <b>Yes</b> to enable the transfer service. Select <b>No</b> to disable it.</li> </ul> <p>Options: Yes and No</p> <p>Default: Yes</p>
Blind Transfer Serv	<p>Blind call transfer service. The user transfers the call without speaking to the caller.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;Blind_Transfer_Serv ua="na"&gt;Yes&lt;/Blind_Transfer_Serv&gt;</pre> </li> <li>In the phone web page, select <b>Yes</b> to enable the transfer service. Select <b>No</b> to disable it.</li> </ul> <p>Options: Yes and No</p> <p>Default: Yes</p>



# Call Forward

To enable call forward, you can enable the feature in two places: on the Voice tab and the User tab of the phone web page.

## Enable Call Forward on Voice Tab

Perform this task if you want to enable call forward for a user.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code. To configure each parameter, see the syntax of the string in the [Parameters for Enable Call Forward on Voice Tab, on page 240](#) table.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

---

- Step 1** Select **Voice > Phone**.
  - Step 2** Under **Supplementary Services**, configure the parameters as described in the [Parameters for Enable Call Forward on Voice Tab, on page 240](#) table.
  - Step 3** Click **Submit All Changes**.
- 

### Related Topics

- [DND and Call Forward Status Sync, on page 206](#)
- [Enable Feature Key Sync, on page 205](#)
- [Enable Call Forward Status Sync via XSI Service, on page 207](#)

## Parameters for Enable Call Forward on Voice Tab

The following table defines the function and usage of Enable Call Forward on Voice Tab parameters in the Supplementary Services section under the Phone tab in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file with XML(cfg.xml) code to configure a parameter.

**Table 36: Parameters for Enable Call Forward on Voice Tab**

Parameter	Description
Cfwd All Serv	<p>Forwards all calls.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;Cfwd_All_Serv ua="na"&gt;Yes&lt;/Cfwd_All_Serv&gt;</pre> </li> <li>In the phone web page, select <b>Yes</b> to forward all calls. Select <b>No</b> to disable it.</li> </ul> <p>Options: Yes and No</p> <p>Default: Yes</p>
Cfwd Busy Serv	<p>Forwards calls only if the line is busy.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;Cfwd_Busy_Serv ua="na"&gt;Yes&lt;/Cfwd_Busy_Serv&gt;</pre> </li> <li>In the phone web page, select <b>Yes</b> to forward calls when the line is busy. Select <b>No</b> to disable it.</li> </ul> <p>Options: Yes and No</p> <p>Default: Yes</p>

Parameter	Description
Cfwd No Ans Serv	<p>Forwards calls only if the line is not answered.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;Cfwd_No_Ans_Serv ua="na"&gt;Yes&lt;/Cfwd_No_Ans_Serv&gt;</pre> </li> <li>In the phone web page, select <b>Yes</b> to forward calls if the line is not answered. Select <b>No</b> to disable it.</li> </ul> <p>Options: Yes and No</p> <p>Default: Yes</p>

## Enable Call Forward on User Tab

Perform the following task to change the call forward settings from the phone web page.

The settings of call forward are synchronized between the phone and the server when one of the following ways is enabled:

- Feature key synchronization (FKS)
- BroadSoft's Extended Services Interface (XSI) Synchronization

To ensure the settings of call forward on the local phone take effect, you need to disable FKS and XSI first. See [Enable Feature Key Sync, on page 205](#) and [Enable Call Forward Status Sync via XSI Service, on page 207](#).

The priority of taking effect for call forward setting in the supported modes is: FKS > XSI > Local.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

Ensure that the call forward setting is enabled on the Voice tab. See [Enable Call Forward on Voice Tab, on page 239](#).

### Procedure

- 
- Step 1** Select **Voice > User**.
- Step 2** In the **Call Forward** section, configure the parameters as described in the [Parameters for Enable Call Forward on User Tab, on page 242](#) table.
- Step 3** Click **Submit All Changes**.
-

## Parameters for Enable Call Forward on User Tab

The following table defines the function and usage of Voice > User > Call Forward in the phone web page. It also defines the syntax of the string that is added in the phone configuration file with XML(cfg.xml) code to configure a parameter.

Except for the parameter "Forward Softkey", other parameters in the following table take effect only when FKS and XSI disabled.

**Table 37: Parameters for Enable Call Forward on User Tab**

Parameter	Description
Cfwd All	<p>Forwards all calls. The setting of this parameter takes precedence over Cfwd Busy and Cfwd No Answer.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;Cfwd_All ua="rw"&gt;No&lt;/Cfwd_All&gt;</pre> </li> <li>In the phone web page, select <b>Yes</b> to forward all calls. Select <b>No</b> to disable it.</li> </ul> <p>Options: Yes and No</p> <p>Default: No</p>
Cfwd All Dest	<p>Specifies the destination to which all calls are forwarded. The destination can be an alphanumeric input, a phone number, or a SIP URI.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;Cfwd_All_Dest ua="rw"&gt;DestinationNumber&lt;/Cfwd_All_Dest&gt;</pre> </li> <li>In the phone web page, enter the destination number in the field.</li> </ul> <p>When you select <b>Yes</b> for Cfwd All, make sure to configure the parameter.</p> <p>Default: Empty</p>

Parameter	Description
Cfwd Busy	<p>Forwards calls only if the line is busy.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;Cfwd_Busy ua="rw"&gt;No&lt;/Cfwd_Busy&gt;</pre> </li> <li>In the phone web page, select <b>Yes</b> to forward calls when the line is busy. Select <b>No</b> to disable it.</li> </ul> <p>Options: Yes and No Default: No</p>
Cfwd Busy Dest	<p>Specifies the destination to which calls are forwarded if the line is busy. The destination can be an alphanumeric input, a phone number, or a SIP URI.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;Cfwd_Busy_Dest ua="rw"&gt;DestinationNumber&lt;/Cfwd_Busy_Dest&gt;</pre> </li> <li>In the phone web page, enter the destination number in the field.</li> </ul> <p>When you select <b>Yes</b> for Cfwd Busy, make sure to configure the parameter. Default: Empty</p>
Cfwd No Answer	<p>Forwards the incoming call only if the call isn't answered.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;Cfwd_No_Answer ua="rw"&gt;No&lt;/Cfwd_No_Answer&gt;</pre> </li> <li>In the phone web page, select <b>Yes</b> to forward the incoming call if the call isn't answered. Select <b>No</b> to disable it.</li> </ul> <p>Options: Yes and No Default: No</p>

Parameter	Description
Cfwd No Ans Dest	<p>Specifies the phone number of destination to which the incoming call is forwarded if the call isn't answered. The destination can be an alphanumeric input, a phone number, or a SIP URI.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="976 569 1479 625">&lt;Cfwd_No_Answer_Dest ua="rw"&gt;DestinationNumber&lt;/Cfwd_No_Answer_Dest&gt;</pre> </li> <li>In the phone web page, enter the destination number in the field.</li> </ul> <p>When you select <b>Yes</b> for Cfwd No Answer, make sure to configure the parameter.</p> <p>Default: Empty</p>
Cfwd No Ans Delay	<p>Assigns a response delay time (in seconds) for the no answer scenario.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="976 1073 1398 1129">&lt;Cfwd_No_Answer_Delay ua="rw"&gt;20&lt;/Cfwd_No_Answer_Delay&gt;</pre> </li> <li>In the phone web page, enter the delay time in the field.</li> </ul> <p>Default: 20</p>

Parameter	Description
Forward Softkey	<p>Controls the scope of the call forward services that the user can set up by a dedicated softkey. Options are:</p> <ul style="list-style-type: none"> <li>• <b>All Cfwds:</b> Allows the user to set up all call forward services, including Call Forward All, Call Forward Busy, and Call Forward No Answer by pressing the <b>Forward</b> softkey. In this setting, the softkey name is <b>Forward</b> for activation and <b>Clr fwd</b> for deactivation.</li> <li>• <b>Only the C fwd All:</b> Allows the user to directly set up the Call Forward All service by pressing the softkey <b>Forward all</b>. The user can still set up all call forward services from the <b>Settings &gt; User preferences &gt; Call preferences &gt; Call forwarding &gt; Call forward settings</b> screen. In this setting, the softkey name is <b>Forward all</b> for activation and <b>Clr fwd all</b> for deactivation.</li> </ul> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>• In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;Forward_Softkey ua="na"&gt;All Cfwds&lt;/Forward_Softkey&gt;</pre></li> <li>• In the phone web page, select the value that determines the scope of the call forward services for the users.</li> </ul> <p><b>Note</b> The parameter takes effect even though FKS, XSI, or FAC is enabled.</p> <p>Default: All Cfwds</p>

## Enable Feature Activation Code Synchronization for Forward All Calls

You can synchronize forwarding all calls feature to the server with a Feature Activation Code (FAC). When you enable this feature, the FAC sends out the star code and the destination number with INVITE to the server.

### Before you begin


Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

## Procedure

---

**Step 1** Select **Voice > Ext (n)**.

**Step 2** In the **Feature Activation Code Sync** field, select **Yes** to enable the feature.

After you enable this feature, your user can press the **Forward** or **Forward all** softkey on the phone and enter the destination contact number. When the user presses the **Call** softkey, a voice message plays to confirm the call forward setting status. After successful configuration, a call forward  icon displays at the top of the phone screen.

The softkey name is different based on the value of the parameter `Forward Softkey`, see [Parameters for Enable Call Forward on User Tab, on page 242](#).

In the phone configuration file with XML(cfg.xml), enter a string in this format:

```
<Feature_Activation_Code_Sync_n_ ua="na">Yes</Feature_Activation_Code_Sync_n_>
```

where, n is the extension number.

Default value: No

Allowed values: Yes or No

**Step 3** Click **Submit All Changes**.

---

## Set Feature Activation Code for the Call Forward All Service

You can set activation code (star code) that can be used to activate or deactivate the call forward all service.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

## Procedure

---

**Step 1** Select **Voice > Regional**.

**Step 2** In the **Vertical Service Activation Codes** section, ensure that the **Cfwd All Act Code** field is set to the value defined by the server. The default value is \*72.

In the phone configuration file with XML(cfg.xml), enter a string in this format:

```
<Cfwd_All_Act_Code ua="na">*72</Cfwd_All_Act_Code>
```

**Step 3** In the **Vertical Service Activation Codes** section, ensure that the **Cfwd All Deact Code** field is set to the value defined by the server. The default value is \*73.

In the phone configuration file with XML(cfg.xml), enter a string in this format:

```
<Cfwd_All_Deact_Code ua="na">*73</Cfwd_All_Deact_Code>
```

**Step 4** Click **Submit All Changes**.

Your user can dial \*72 in combination with the destination number and press the **Call** softkey to activate the call forward all service.



Your user can dial \*73 and press the **Call** softkey to deactivate the call forward all service.

## Enable Conferencing

You can enable your user to talk to several people in a single call. When you enable this feature, your user dials several people and add them to the call.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

**Step 1** Select **Voice > Phone**.

**Step 2** Under **Supplementary Services**, choose **Yes** for the **Conference Serv** parameter.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<Conference_Serv ua="na">Yes</Conference_Serv>
```

Options: Yes and No

Default: Yes

**Step 3** Click **Submit All Changes**.

## Enable Remote Call Recording with SIP REC

You can enable call recording on a phone so that your user can record an active call. The recording mode configured on the server controls the display of the recording softkeys for each phone.

**Table 38: Recording Mode and Recording Softkeys**

Recording Mode in Server	Recording Softkeys Available on the Phone
Always	No softkeys available. Your user can't control recording from the phone. Recording starts automatically when a call is connected.
Never	PauseRec ResumeRec When a call is connected, recording starts automatically and your user can control the recording.

Recording Mode in Server	Recording Softkeys Available on the Phone
On Demand	Record PauseRec ResumeRec  When a call is connected, recording starts automatically but the recording is not saved until the user presses the <b>Record</b> softkey. Your user sees a message when recording state changes.
On Demand with User Initiated Start	Record PauseRec StopRec ResumeRec  The recording only starts when your user presses the <b>Record</b> softkey. Your user sees a message when recording state changes.

During a recording, your user sees different icons which depend on the recording state. The icons are displayed on the Calls screen and also on the line key on which the user is recording a call.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

**Step 1** Select **Voice > Phone**.

**Step 2** In the **Supplementary Services** section, click **Yes** or click **No** to enable or to disable the **Call Recording Serv** parameter.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<Call_Recording_Serv ua="na">Yes</Call_Recording_Serv>
```

Options: Yes and No

Default: No

**Step 3** (Optional) In the **Programmable Softkeys** section, to enable softkeys, add a string in this format in the **Connected Key List** and **Conferencing Key List** fields.

```
crdstart;crdstop;crdpause;crdresume
```

**Step 4** Click the **Ext(n)** tab that requires call recording.

**Step 5** In the **SIP Settings** section, in the **Call Recording Protocol**, select **SIPREC** as the call recording protocol.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<Call_Recording_Protocol_3_ ua="na">SIPREC</Call_Recording_Protocol_3_>
```

Options: SIPREC and SIPINFO

Default: SIPREC

**Step 6** Click **Submit All Changes**.

---

## Enable Remote Call Recording with SIP INFO

You can enable call recording on a phone so that your user can record an active call.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code.

During a recording, your user sees different icons which depend on the recording state. The icons are displayed on the Calls screen and also on the line key on which the user is recording a call.

Your user presses the following softkeys to control the phone recording:

- **Record**
- **StopRec**

The recording only starts when your user presses the **Record** softkey. Your user sees a message when recording state changes and the recording icon displays on the call screen.

Once a phone recording starts, the **StopRec** softkey can work. The recording stops when your user presses the **StopRec** softkey. Your user sees a message when the recording state changes.

### Before you begin

- You need to set up call recording on the call control system.
- Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

---

**Step 1** Select **Voice > Phone**.

**Step 2** In the **Supplementary Services** section, click **Yes** or click **No** to enable or to disable call recording in the **Call Recording Serv** parameter.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<Call_Recording_Serv ua="na">Yes</Call_Recording_Serv>
```

Options: Yes and No

Default: No

**Step 3** (Optional) In the **Programmable Softkeys** section, to enable softkeys, add a string in this format in the **Connected Key List** and **Conferencing Key List** fields.

```
crdstart;crdstop;crdpause;crdresume
```

**Step 4** Click the **Ext(n)** tab that requires call recording.

**Step 5** In the **SIP Settings** section, for the **Call Recording Protocol** parameter, select **SIPINFO** as the call recording protocol.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<Call_Recording_Protocol_1_ ua="na">SIPINFO</Call_Recording_Protocol_1_>
```

Options: SIPREC and SIPINFO

Default: SIPREC

**Step 6** Click **Submit All Changes**.

---

## Configure Missed Call Indication

You can configure a missed call alert on the phone handset LED.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

---

**Step 1** Select **Voice > User**.

The user can select **User Login > Voice > User**.

**Step 2** In the **Supplementary Services** section, for the **Handset LED Alert** parameter, select **Voicemail, Missed Call**.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<Handset_LED_Alert ua="rw">Voicemail,Missed Call</Handset_LED_Alert>
```

Options: Voicemail and Voicemail, Missed Call

Default: Voicemail

**Step 3** Click **Submit All Changes**.

---

## Enable Do Not Disturb

You can allow persons to turn the Do not disturb feature on or off. The caller receives a message that the person is unavailable. A person can press the **Ignore** softkey on the phone to divert an incoming call to another destination.

If the feature is enabled for the phone, users can turn the feature on or off with the DND softkey.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

---

**Step 1** Select **Voice > User**.

**Step 2** In the **Supplementary Services** area, for the **DND Setting** parameter, select **Yes**.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<DND_Setting ua="rw">Yes</DND_Setting>
```

Options: Yes and No

Default: No

**Step 3** Click **Submit All Changes**.

---

When you select a line (multiline phone), a Do Not Disturb banner displays at the top of the phone screen.

### What to do next

Change another setting to ensure that multiline phones correctly display the Do not disturb (currently, a steady, green color) status for each selected or unselected line. See [DND and Call Forward Status Sync, on page 206](#).

Users can enable or turn off the DND feature for each phone line if you configure star codes for DND. See [Configure Star Codes for DND, on page 255](#).

### Related Topics

[DND and Call Forward Status Sync, on page 206](#)

[Enable Feature Key Sync, on page 205](#)

[Enable DND Status Sync via XSI Service, on page 208](#)



## Enable Synchronization of Settings Between the Phone and the Server

Enable the synchronization of settings between the phone and the server.

This setting must be enabled for the following features and types of users:

- Call forward all
- DND

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code.

If a line key is configured with feature key sync and is also enabled with DND or call forward feature, the respective DND  or the call forward  icon is displayed next to the line key label. If the line key has a missed call, a voice message, or an urgent voicemail alert, the DND icon or the call forward icon is also displayed with the alert notification.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

---

**Step 1** Select **Voice > Ext [n]** (where [n] is the extension number).

**Step 2** In the **Call Feature Settings** section, set the **Feature Key Sync** parameter to **Yes**.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<!-- Call Feature Settings -->
<Feature_Key_Sync_1_ ua="na">Yes</Feature_Key_Sync_1_>
```

Options: Yes and No

Default: No

**Step 3** Click **Submit All Changes**.

---

## Enable Webex Contacts on the Phone

When you onboard a phone to Webex cloud successfully, you can enable the phone to support Webex contacts. When you enable this feature on the phone, your user can see the Webex directory under the phone directory list.

When you configure **Max Display Records** parameter value more than 100, the query result displays only hundred contacts for a search in Webex directory and All directory. When search result has count more than the allowed display record value, user see a message: Too many matches found. Refine your search. For more information on **Max Display Records** parameter, see [Parameters for Directory Services, on page 297](#).

### Before you begin

- Phone onboards to Cisco Webex cloud successfully. For more information on phone onboarding to Webex Cloud, see [Webex for Cisco BroadWorks Solution Guide](#).
- Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

---

**Step 1** Select **Voice > Phone**.

- Step 2** In the **Webex** section, set the **Directory Enable** to **Yes**.
- You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:
- ```
<Webex_Directory_Enable ua="na">Yes</Webex_Directory_Enable>
```
- Default value: No
- Step 3** In the **Directory Name** field, enter a name for the Webex directory.
- You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:
- ```
<Webex_Directory_Name ua="na">wkdir</Webex_Directory_Name>
```
- Default value: Empty
- The name you enter (for example, **wkdir** ), displays as the Webex directory name on the phone under the directory list. You can modify this name from the phone administration web page or from the configuration XML file string. When required, your user can also modify this name from the phone. When the **Directory Name** field is empty, by default, the Webex directory name on the phone appears as **Webex directory**.
- When the phone is not onboarded to Cisco Webex cloud successfully, the **Webex directory** doesn't appear under the directory list.
- Step 4** Click **Submit All Changes**.
- 

## Configure Webex Contacts on a Line Key

You can configure Webex contacts on a line key. This line key becomes a shortcut to the Webex directory.

### Before you begin

- Phone onboards to Cisco Webex cloud successfully.
- Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).
- **Directory Enable** on the phone administration web page is set to **Yes**.

### Procedure

---

- Step 1** Select **Voice > Phone**.
- Step 2** Select a line key.
- Step 3** Set the **Extension** field to **Disabled**.
- Step 4** In the **Extended Function** parameter, enter a string in this format:
- ```
fnc=shortcut;url=webexdir;nme=cloudplk
```
- where fnc=shortcut means function=shortcut, url is the menu to open this line key, and nme is the name for the Webex directory.

In the string, when `nme` is empty or you don't include `nme` in the string, by default, the line key displays the directory name as **Webex directory**.

You can also configure this parameter in the configuration file (cfg.xml). Enter a string in this format:

```
<Extended_Function_n_ua="na">fnc=shortcut;url=webexdir;nme=cloudplk</Extended_Function_n_>
```

where `n` is the extension number.

The line key is configured with the feature. For example, if you assign the feature in line key number nine, the user sees **cloudplk** appears in the line number nine as a shortcut to the Webex directory. By pressing this configured line key, user can access the **Search Webex directory** screen and can search the Webex contacts.

If **Directory Enable** on the phone administration web page is set to **No**, the line key doesn't work.

If the phone is not onboarded to the Webex cloud successfully, the line key doesn't work.

**Step 5** Click **Submit All Changes**.

## Add a Softkey for Webex Contacts

You can configure Webex contacts to a softkey. This softkey becomes a shortcut to the Webex directory.

### Before you begin

- Phone onboarded to Cisco Webex cloud successfully.
- Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).
- **Directory Enable** on the phone administration web page is set to **Yes**.

### Procedure

**Step 1** Select **Voice > Phone**.

**Step 2** In the **Programmable Softkeys** section, set the **Programmable Softkey Enable** to **Yes**.

**Step 3** Configure a PSK field from PSK 1 through PSK 16 with a string in this format:

```
fnc=shortcut;url=webexdir;nme=cloudplk
```

You can also configure this parameter in the configuration file (cfg.xml). Enter a string in this format:

```
<PSK_n_ua=na>fnc=shortcut;url=webexdir;nme=cloudplk</PSK_n>
```

A softkey is configured with the feature and appears on the phone. For example, **cloudplk** appears as a softkey and acts as a shortcut to the Webex directory. By pressing this softkey, user can access the **Search Webex directory** screen and can search the Webex contacts.

In the string, when `nme` is empty or you don't include `nme` in the string, by default, the softkey displays the directory name as **Webex Dir**.

If **Directory Enable** on the phone administration web page is set to **No**, the softkey doesn't work.



If the phone is not onboarded to Cisco Webex cloud successfully, the softkey doesn't work.

---

## Enable Webex Call Logs on the Phone

You can now enable a phone to support Webex call logs. When you enable this feature, the **Display recents from** menu under the **Recents** screen includes the **Webex** option in the calls list. The user then can set the option **Webex** to see the list of recent Webex calls.

### Before you begin

- Phone onboards to Webex cloud successfully. For more information on phone onboarding to Webex cloud, see [Webex for Cisco BroadWorks Solution Guide](#).
- Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).
- Under the **Call Log** section, enable the **CallLog Enable** parameter and select a phone line from **CallLog Associated Line** for which you want to display the Webex recent call logs.

### Procedure

---

**Step 1** Select **Voice > Phone**.

**Step 2** In the **Call Log** section, set the **CallLog Enable** parameter to **Yes** and **Display Recents From** parameter to **Webex**.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<CallLog_Enable ua="na">Yes</CallLog_Enable>
<Display_Recents_From ua="na">Webex</Display_Recents_From>
```

Default value of **Display Recents From** : Phone

**Step 3** Click **Submit All Changes**.

---

## Configure Star Codes for DND

You can configure star codes that a user dials to turn on or off the do not disturb (DND) feature on a phone. You can also configure the parameters in the phone configuration file with XML(cfg.xml) code.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

---

**Step 1** Select **Voice > Regional**.

**Step 2** In the **Vertical Service Activation Codes** section, enter \*78 for the **DND Act Code** parameter.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<DND_Act_Code ua="na">*78</DND_Act_Code>
```

**Step 3** In the **Vertical Service Activation Codes** section, enter \*79 for the **DND Deact Code** parameter.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<DND_Deact_Code ua="na">*79</DND_Deact_Code>
```

**Step 4** Click **Submit All Changes**.

---

## Set Up a Call Center Agent Phone

You can enable a phone with Automatic Call Distribution (ACD) features. This phone acts as a call center agent's phone and can be used to trace a customer call, to escalate any customer call to a supervisor in emergency, to categorize contact numbers using disposition codes, and to view customer call details.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code. To configure each parameter, see the syntax of the string in the [Parameters for Call Center Agent Setup, on page 257](#) table.

### Before you begin

- Set up the phone as a call center phone on the BroadSoft server.
- Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

---

**Step 1** Select **Voice > Ext(n)**.

**Step 2** In the **ACD Settings** section, set up the fields as described in [Parameters for Call Center Agent Setup, on page 257](#) table.

**Step 3** Click **Submit All Changes**.

---

## Parameters for Call Center Agent Setup

The following table defines the function and usage of Call Center Agent Setup parameters in the ACD Settings section under the Ext(n) tab in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file with XML(cfg.xml) code to configure a parameter.

**Table 39: Parameters for Call Center Agent Setup**

| Parameter               | Description   |
|-------------------------|---|
| Broadsoft ACD           | <p>Enables the phone for Automatic Call Distribution (ACD).</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;Broadsoft_ACD_1_ua="na"&gt;Yes&lt;/Broadsoft_ACD_1_&gt;</pre> </li> <li>In the phone web page, select <b>Yes</b> to enable this feature and select <b>No</b> to disable it.</li> </ul> <p>Options: Yes and No<br/>Default: No</p>                      |
| Call Information Enable | <p>Enables the phone to display details of a call center call.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;Call_Information_Enable_1_ua="na"&gt;Yes&lt;/Call_Information_Enable_1_&gt;</pre> </li> <li>In the phone web page, select <b>Yes</b> to enable this feature. Select <b>No</b> to disable it.</li> </ul> <p>Options: Yes and No<br/>Default: Yes</p> |

| Parameter                   | Description  |
|-----------------------------|--|
| Disposition Code Enable     | <p>Enables the user to add a disposition code.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="976 474 1479 527">&lt;Disposition_Code_Enable_1_ua="na"&gt;Yes&lt;/Disposition_Code_Enable_1_&gt;</pre> </li> <li>In the phone web page, select <b>Yes</b> to enable this feature. Select <b>No</b> to disable it.</li> </ul> <p>Options: Yes and No<br/>Default: Yes</p>   |
| Trace Enable                | <p>Enables the user to trace the last incoming call.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="976 919 1349 972">&lt;Trace_Enable_1_ua="na"&gt;Yes&lt;/Trace_Enable_1_&gt;</pre> </li> <li>In the phone web page, select <b>Yes</b> to enable this feature. Select <b>No</b> to disable it.</li> </ul> <p>Options: Yes and No<br/>Default: Yes</p>   |
| Emergency Escalation Enable | <p>Enables the user to escalate a call to a supervisor in case of emergency.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="976 1392 1479 1444">&lt;Emergency_Escalation_Enable_1_ua="na"&gt;Yes&lt;/Emergency_Escalation_Enable_1_&gt;</pre> </li> <li>In the phone web page, select <b>Yes</b> to enable this feature. Select <b>No</b> to disable it.</li> </ul> <p>Options: Yes and No<br/>Default: Yes</p> |

| Parameter                        | Description   |
|----------------------------------|---|
| Queue Status Notification Enable | <p>Displays the call center status and the agent status.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;Queue_Status_Notification_Enable_1_ua="na"&gt;Yes&lt;/Queue_Status_Notification_Enable_1_&gt;</pre> </li> <li>In the phone web page, select <b>Yes</b> to enable this feature. Select <b>No</b> to disable it.</li> </ul> <p>Options: Yes and No<br/>Default: Yes</p>   |
| Auto Available After Sign-In     | <p>Sets the agent status to Available automatically when the user signs into the phone as a call center agent.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;Auto_Available_After_Sign-In_1_ua="na"&gt;Yes&lt;/Auto_Available_After_Sign-In_1_&gt;</pre> </li> <li>In the phone web page, select <b>Yes</b> to enable this feature and select <b>No</b> to disable it.</li> </ul> <p>Options: Yes and No<br/>Default: No</p> |

## Restore the ACD Status

You can enable the phone to automatically set the ACD status to the last local value in one of the following situations:

- Phone is powered on.
- Phone status is changed to “Registered” from “Unregistered” or “Registration failed” status.
- Registration destination server IP address is changed when failover happens, a fallback happens, or a DNS response is changed.

### Before you begin

- Set up the phone as a call center phone on the BroadSoft server.
- Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

---

**Step 1** Select **Voice > Ext(n)**.

**Step 2** In the **ACD Settings** section, set **BraodSoft ACD** to **Yes**.

**Step 3** From **ACD Status** field, select one of the options:

- **Sync From Local:** Select this option to restore the last local status as ACD status when the phone boots up, status is changed to "Registered" from "Unregistered" or "Registration failed", or registration destination ip address is changed due to failover, fallback or DNS response is changed.

When the intial ACD status is configured to sync from local, and the last local status is unavailable with a reason code, after the phone boots up, the reason code will not be restored.

- **Sync From Server:** Select this option to get ACD intial status from the server. This is the default value.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<ACD_Status_n_ ua="na">Sync From Local</ACD_Status_n_>
```

where n = 1 to 16

**Step 4** Click **Submit All Changes**.

---

## Display or Hide Unavailable Menu Text Box of Agent Status on the Phone

You can control if your user wants to hide the **Unavailable** menu text box of the **Set agent status** screen on the phone.

### Before you begin

- Set up the phone as a call center phone on the BroadSoft server.
- Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

---

**Step 1** Select **Voice > Ext(n)**.

**Step 2** In the **ACD Settings** section, set the **Unavailable Reason Code Enable** parameter to **No** to hide the **Unavailable** text box on the phone.

To display the text box, select **Yes**. This is the default value.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<Unavailable_Reason_Code_Enable_1_ ua="na">Yes</Unavailable_Reason_Code_Enable_1_>
```

**Step 3** Click **Submit All Changes**.

---

# Set Up a Phone for Presence

You can enable the BroadSoft XMPP directory for the phone user.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code. To configure each parameter, see the syntax of the string in the [Parameters for Set Up Presence, on page 261](#) table.

## Before you begin

- Set up the BroadSoft server for XMPP.
- Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

## Procedure

- 
- Step 1** Select **Voice > Phone**.
- Step 2** In the **Broadsoft XMPP** section, set the fields as described in the [Parameters for Set Up Presence, on page 261](#).
- Step 3** Click **Submit All Changes**.
- 

## Parameters for Set Up Presence

The following table defines the function and usage of Set Up Presence parameters in the Broadsoft XMPP section under the Phone tab in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file with XML(cfg.xml) code to configure a parameter.

*Table 40: Parameters for Set Up Presence*

| Parameter   | Description   |
|-------------|---|
| XMPP Enable | <p>Enables the BroadSoft XMPP directory for the phone user.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>• In the phone configuration file with XML(cfg.xml), enter a string in this format:<br/> <pre>&lt;XMPP_Enable ua="na"&gt;Yes&lt;/XMPP_Enable&gt;</pre> </li> <li>• In the phone web page, select <b>Yes</b> to forward all calls. Select <b>No</b> to disable it.</li> </ul> <p>Options: Yes and No<br/>Default: No</p> |

| Parameter | Description   |
|-----------|---|
| Server    | <p>Name of the XMPP server; for example, xsi.iop1.broadworks.net.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="976 506 1481 562">&lt;XMPP_Server ua="na"&gt;xsi.iop1.broadworks.net&lt;/XMPP_Server&gt;</pre> </li> <li>In the phone web page, enter a name for the server.</li> </ul> <p>Default: Empty</p>   |
| Port      | <p>Server port for the XMPP server.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="976 898 1422 926">&lt;XMPP_Port ua="na"&gt;5222&lt;/XMPP_Port&gt;</pre> </li> <li>In the phone web page, enter the server port.</li> </ul> <p>Allowed values: An integer from 0 through 65535</p> <p>If the value is set to 0, the phone first sends a DNS SRV query for the domain (specified in <b>Server</b> or <b>User ID</b>) to obtain the XMPP server IP address. If there is no A record in the DNS SRV response, then the phone sends as fallback an A record lookup for the same domain to obtain the IP address. In this scenario, the actual port number is 5222.</p> <p><b>Note</b> When both <b>Server</b> and <b>User ID</b> contain the domain names, the domain name in <b>Server</b> is preferred.</p> <p>If the value isn't set to 0, the phone directly sends an A record lookup for the domain (specified in <b>Server</b> or <b>User ID</b>) to obtain the XMPP server IP address.</p> <p>Default: 5222</p> |



| Parameter       | Description   |
|-----------------|---|
| User ID         | <p>BroadSoft User ID of the phone user; for example, username1@xdp.broadsoft.com or username1.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="1013 506 1422 562">&lt;XMPP_User_ID ua="na"&gt;username1&lt;/XMPP_User_ID&gt;</pre> </li> <li>In the phone web page, enter the user ID.</li> </ul> <p>If the value doesn't contain the domain name, the phone first generates a new user ID by combining the values of this parameter and <b>Server</b>. For example, the server is xsi.iop1.broadworks.net and user ID is username1, the generated user ID is username1@xsi.iop1.broadworks.net.</p> <p>Then, the phone sends A record lookup or DNS SRV query for the domain xsi.iop1.broadworks.net to obtain the XMPP server IP address.</p> <p>Default: Empty</p> |
| Password        | <p>Alphanumeric password associated with the User ID.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="1013 1184 1511 1209">&lt;XMPP_Password ua="na"&gt;&lt;/XMPP_Password&gt;</pre> </li> <li>In the phone web page, enter a supported password.</li> </ul> <p>Default: Empty</p>  |
| Login Invisible | <p>When enabled, the user's presence information is not published when the user signs in.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="1013 1583 1382 1640">&lt;Login_Invisible ua="na"&gt;Yes&lt;/Login_Invisible&gt;</pre> </li> <li>In the phone web page, select Yes to enable the feature.</li> </ul> <p>Options: Yes and No</p> <p>Default: No</p>   |

| Parameter   | Description   |
|-------------|---|
| Retry Intvl | <p>Interval, in seconds, to allow a reconnect without a log in after the client disconnects from the server. After this interval, the client needs to reauthenticate.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;Login_Invisible ua="na"&gt;Yes&lt;/Login_Invisible&gt;</pre> </li> <li>In the phone web page, select Yes to enable the feature.</li> </ul> <p>Options: Yes and No</p> <p>Default: No</p> |

## Configure the Number of Call Appearances Per Line

Phones that support multiple call appearances on a line can be configured to specify the number of calls to allow on the line.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

- 
- Step 1** Select **Voice > Phone**.
- Step 2** In the **Miscellaneous Line Key Settings** section, for the **Call Appearances Per Line** parameter, specify the number of calls per line to allow.
- You can also configure this parameter in the configuration file (cfg.xml) by entering a string in this format:
- ```
<Call_Appearances_Per_Line ua="na">2</Call_Appearances_Per_Line>
```
- The allowed values range from 2 to 10. The default value is 2.
- Step 3** Click **Submit All Changes**.
- 

## Enable Reverse Name Lookup

Reverse name lookup searches for the name of a number in an incoming, outgoing, conference, or transferred call. The reverse name lookup acts when the phone cannot find a name using the service provider directory,

Call History, or your contacts. Reverse name lookup needs a valid BroadSoft (XSI) Directory, LDAP Directory, or XML Directory configuration.

The reverse name lookup searches the phone's external directories. When a search succeeds, the name is placed in the call session and in the call history. For simultaneous, multiple phone calls, reverse name lookup searches for a name to match the first call number. When the second call connects or is placed on hold, reverse name lookup searches for a name to match the second call. The reverse lookup searches the external directories for 8 secs, if in 8secs there are no results found, there will be no display of the name. If results are found in 8secs, the name is displayed on the phone. The external directory search priority order is : **BroadSoft (XSI) > LDAP > XML**.

While searching if the lower priority name is received before the higher priority name, the search shows the lower priority name first and then replaced it with the higher priority name if the higher priority name is found within 8 secs.

The precedence of the phone list lookup in BroadSoft (XSI) Directory is:

1. Personal phone list
2. Group common phone list
3. Enterprise common phone list

Reverse name lookup is enabled by default.

Reverse name lookup searches the directories in the following order:

1. Personal Address Book
2. SIP Header
3. Call History
4. BroadSoft (XSI) Directory
5. LDAP Directory
6. XML Directory



---

**Note** The phone searches the XML directory using this format: `directory_url?n=incoming_call_num`

Example: For a multiplatform phone using a third-party service, the phone number (1234) search query is in this format, `http://your-service.com/dir.xml?n=1234`.

---

### Before you begin

- Configure one of these directories before you can enable or disable the reverse name lookup:
  - BroadSoft (XSI) Directory
  - LDAP Corporate Directory
  - XML Directory
- Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

## Procedure

---

- Step 1** Select **Voice > Phone**.
- Step 2** In the **Supplementary Services** area, set the **Reverse Phone Lookup Serv** parameter to **Yes** to enable this feature.
- You can also configure this parameter in the configuration file (cfg.xml) by entering a string in this format:
- ```
<Reverse_Phone_Lookup_Serv ua="na">Yes</Reverse_Phone_Lookup_Serv>
```
- The allowed values are Yes|No. The default value is Yes.
- Step 3** Click **Submit All Changes**.
- 

# Emergency Calls

## Emergency Call Support Background

Emergency call service providers can register a phone's location for each IP-based phone in a company. The location information server (LIS) transfers the emergency response location (ERL) to the phone. The phone stores its location during registration, after the phone restarts, and when a person signs in to the phone. The location entry can specify the street address, building number, floor, room, and other office location information.

When you place an emergency call, the phone transfers the location to the call server. The call server forwards the call and the location to the emergency call service provider. The emergency call service provider forwards the call and a unique call-back number (ELIN) to the emergency services. The emergency service or public safety answering point (PSAP) receives the phone location. The PSAP also receives a number to call you back, if the call disconnects.

See [Emergency Call Support Terminology, on page 267](#) for the terms used to describe emergency calls from the phone.

You insert the following parameters to obtain the phone's location for any phone extension number:

- **Company Identifier**—A Unique number (UUID) assigned to your company by the NG9-1-1 service provider.
- **Primary Request URL**—The HTTPS address of the primary server used to obtain the phone location.
- **Secondary Request URL**—The HTTPS address of a secondary server (backup) used to obtain the phone location.
- **Emergency Number**—A sequence of digits that identify an emergency call. You can specify multiple emergency numbers, by separating each emergency number with a comma.

Common emergency service numbers include:

- North America—911
- European countries—112
- Hong Kong—999

The phone requests new location information for the following activities:

- You register the phone with the call server.
- A person restarts the phone and the phone was previously registered with the call server.
- A guest signs in to the phone.
- You change the IP address of the phone.

If all of the location servers do not send a location response, the phone re-sends the location request every two minutes.

## Emergency Call Support Terminology

The following terms describe emergency call support for the Cisco Multiplatform Phones.

- **Emergency Location ID Number (ELIN)**—A number used to represent one or more phone extensions that locate the person who dialed emergency services.
- **Emergency Response Location (ERL)**—A logical location that groups a set of phone extensions.
- **HTTP Enabled Location Delivery (HELD)**—An encrypted protocol that obtains the PIDF-LO location for a phone from a location information server (LIS).
- **Location Information Server (LIS)**—A server that responds to a SIP-based phone HELD request and provides the phone location using a HELD XML response.
- **Emergency Call Service Provider**—The company that responds to a phone HELD request with the phone's location. When you make an emergency call (which carries the phone's location), a call server routes the call to this company. The emergency call service provider adds an ELIN and routes the call to the emergency services (PSAP). If the call is disconnected, the PSAP uses the ELIN to reconnect with the phone used to make the emergency call.
- **Public Safety Answering Point (PSAP)**—Any emergency service (for example, fire, police, or ambulance) joined to the Emergency Services IP Network.
- **Universally Unique Identifier (UUID)**—A 128-bit number used to uniquely identify a company using emergency call support.

## Configure a Phone to Make Emergency Calls

### Before you begin

- Obtain the E911 Geolocation Configuration URLs and the company identifier for the phone from your emergency call services provider. You can use the same Geolocation URLs and company identifier for multiple phone extensions in the same office area.
- Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

## Procedure

---

- Step 1** Select **Voice > Ext  $n$** , where  $n$  is the phone extension number (1-10) of the phone web dialog.
- Step 2** In the **Dial Plan** section, set the **Emergency Number** parameter
- Step 3** In the **E911 Geolocation Configuration** section, set the **Company UUID**, **Primary Request URL**, and **Secondary Request URL** parameters as described in the [Parameters to Make an Emergency Call](#), on page 268.
- Step 4** Click **Submit All Changes**.
- 

## Parameters to Make an Emergency Call

The following table defines the function and usage of Making of Emergency Calls parameters in the Dial Plan and E911 Geolocation Configuration sections under the Ext( $n$ ) tab in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file with XML(cfg.xml) code to configure a parameter.

*Table 41: Parameters to Make an Emergency Call*

| Parameter                 | Description |
|---------------------------|-------------|
| <b>Section: Dial Plan</b> |             |

| Parameter                                      | Description   |
|--|---|
| Emergency Number                               | <p>Enter a comma-separated list of emergency numbers.</p> <p>To specify multiple emergency numbers, separate each emergency number with a comma.</p> <p>When one of these numbers is dialed, the unit disables processing of CONF, HOLD, and other similar softkeys or buttons to avoid accidentally putting the current call on hold. The phone also disables hook flash event handling.</p> <p>Only the far end can terminate an emergency call. The phone is restored to normalcy after the call is terminated and the receiver is back on-hook.</p> <p>Perform one of the following: to the digits that correspond to the customer emergency service numbers.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="1015 898 1398 926">&lt;Emergency_Number_1_ ua="na"/&gt;</pre> </li> <li>In the phone web page, set <b>Emergency Number</b> parameter to the digits that correspond to the customer emergency service numbers.</li> </ul> <p>Valid Values: Maximum number length is 63 characters</p> <p>Default: Blank (no emergency number)</p> |
| <b>Section: E911 Geolocation Configuration</b> |   |
| Company UUID                                   | <p>The Universally Unique Identifier (UUID) assigned to the customer by the emergency call services provider.</p> <p>For example:</p> <pre data-bbox="963 1409 1523 1436">07072db6-2dd5-4aa1-b2ff-6d588822dd46</pre> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="1015 1591 1349 1619">&lt;Company_UUID_1_ ua="na"/&gt;</pre> </li> <li>In the phone web page, enter a valid identifier assigned by the call services provider.</li> </ul> <p>Valid Values: Maximum identifier length is 128 characters.</p> <p>Default: Blank</p>   |





| Parameter             | Description   |
|-----------------------|---|
| Primary Request URL   | <p>Encrypted HTTPS phone location request. The request uses the phone IP addresses, MAC address, Network Access Identifier (NAI), and chassis ID and port ID assigned by the network switch manufacturer. The request also includes the location server name and the customer identifier.</p> <p>The server used by the emergency call services provider responds with an Emergency Response Location (ERL) that has a location Uniform Resource Identifier (URI) tied to the user phone IP address.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;Primary_Request_URL_1_ua="na"/&gt;</pre> </li> <li>In the phone web page, enter encrypted HTTPS phone location request.</li> </ul> <p>For example:</p> <pre>https://pro2.blueearth.com/911locate/held/held_request.action</pre> <p>Default: Blank</p> |
| Secondary Request URL | <p>Encrypted HTTPS request sent to the emergency call services provider's backup server to obtain the user's phone location.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;Secondary_Request_URL_1_ua="na"/&gt;</pre> </li> <li>In the phone web page, enter the encrypted for the backup server that can return location information.</li> </ul> <p>For example:</p> <pre>https://pro2.blueearth.com/911locate/held/held_request.action</pre> <p>Default: Blank</p>   |

## Spam Indication for Incoming Webex Calls

To support a spam indication for the incoming calls in Webex environment, server sends the `X-Cisco-CallerId-Disposition` disposition information to the phone. The phone translates this information as authentication icons. Based on the caller's STIR/SHAKEN verification result, the phone displays three



types of icons. The icons are displayed next to the caller ID for call session, local call logs, Webex cloud call logs.

- Validated call - The server sends the disposition information, `X-Cisco-CallerId-Disposition=valid`, to the phone. The phone displays an extra icon  next to the caller ID with a color screen indicating a validated caller. For a phone with grayscale screen, an extra icon  next to the caller ID is displayed.
- Invalidated or Spam call - The server sends the disposition information, `X-Cisco-CallerId-Disposition=invalid`, to the phone. The phone displays an extra icon  next to the caller id indicating an illegitimate caller.
- Unverified call - The server sends the disposition information, `X-Cisco-CallerId-Disposition=unverified`, to the phone. The phone displays an extra icon  next to the caller id indicating an unverified call.

When there is no disposition information, the phone displays the same icons as before.

## Programmable Softkeys Configuration

### Customize Display of the Softkeys

You can customize display of the softkeys on the phone screen during a specific state.

You can also configure the parameters in the phone configuration file with XML (cfg.xml) code. To configure each parameter, see the syntax of the string in [Parameters for Programmable Softkeys, on page 271](#).

#### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

#### Procedure

- 
- Step 1** Select **Voice > Phone**.
  - Step 2** In the **Programmable Softkeys** section, edit the softkeys depending on the call state that you want the softkey to display. For more information, see [Parameters for Programmable Softkeys, on page 271](#) and .
  - Step 3** Click **Submit All Changes**.
- 

### Parameters for Programmable Softkeys

The following table defines the function and usage of the programmable softkeys parameters in the **Programmable Softkeys** section under the **Voice > Phone** tab in the phone web interface. It also defines the

syntax of the string that is added in the phone configuration file (cfg.xml) with the XML code to configure a parameter.

**Table 42: Parameters for Programmable Softkeys**

| Parameter                   | Description and default value  |
|-----------------------------|--|
| Programmable Softkey Enable | <p>Enables or disables the programmable softkeys. Set this field to <b>Yes</b> to enable the programmable softkeys.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:           <pre>&lt;Programmable_Softkey_Enable ua="na"&gt;Yes&lt;/Programmable_Softkey_Enable&gt;</pre> </li> <li>In the phone web interface, set this field to <b>Yes</b> or <b>No</b> to enable or disable the programmable softkeys.</li> </ul> <p>Allowed values: Yes   No</p> <p>Default: No</p>  |
| PSK 1 through PSK 16        | <p>Programmable softkey fields. Enter a string in these fields to configure softkeys that display on the phone screen. You can create softkeys for speed dials to numbers or extensions, vertical service activation codes (* codes), or XML scripts.</p> <p>Configure the PSKs in this format:</p> <ul style="list-style-type: none"> <li>Speed Dial:           <pre>fnc=sd;ext=extension_number@\$PROXY;vid=n;nme=display_name</pre> </li> <li>Vertical Service Activation Code:           <pre>fnc=sd;ext=star_code@\$PROXY;vid=n;nme=display_name</pre> <p>See <a href="#">Vertical Service Activation Codes, on page 417</a>.</p> </li> <li>XML Service:           <pre>fnc=xml;url=http://server_IP/services.xml;vid=n;nme=display_name</pre> </li> </ul> <p>When you add a programmable softkey to a softkey list, such as Idle Key List, Missed Call Key List, and so on, the programmable softkey displays on the phone screen.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:           <pre>&lt;PSK_1 ua="na"&gt;fnc=xml;url=http://server_IP/services.xml;vid=n;nme=display_name&lt;/PSK_1&gt;</pre> </li> <li>In the phone web interface, set the PSKs in the valid format.</li> </ul> <p>Default: Empty</p> |

## Customize a Programmable Softkey

The phone provides sixteen programmable softkeys (fields PSK1 through PSK16). You can define the fields by a speed-dial script.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

---

- Step 1** Select **Voice > Phone**.
  - Step 2** In the **Programmable Softkeys** section, set the **Programmable Softkey Enable** to **Yes**.
  - Step 3** Select a programmable softkey number field on which to configure a phone feature.
  - Step 4** Enter the string for the programmable soft key. See the different types of programmable softkeys described in [Configure Speed Dial on a Programmable Softkey, on page 273](#).
  - Step 5** Click **Submit All Changes**.
- 

## Configure Speed Dial on a Programmable Softkey

You can configure programmable softkeys as speed dials. The speed dials can be extensions or phone numbers. You can also configure programmable softkeys with speed dials that perform an action that a vertical service activation code (or a star [\*] code) defines. For example, if you configure a programmable softkey with a speed dial for \*67, the call is placed on hold.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

---

- Step 1** Select **Voice > Phone**.
- Step 2** In the **Programmable Softkeys** section, set the **Programmable Softkey Enable** to **Yes**.
- Step 3** To configure a speed dial PSK, enter the following in the PSK **number** field:

```
fnc=sd;ext=extensionname/starcode@$PROXY;vid=n;nme=name
```

Where:

- fnc= function of the key (speed dial)
- extensionname=extension being dialed or the star code action to perform
- vid= n is the extension that the speed dial will dial out
- name is the name of the speed dial being configured

**Note** The **name** field displays on the softkey on the IP phone screen. We recommend a maximum of 10 characters for a phone. If more characters are used, the label might be truncated on the phone screen.

**Step 4** Edit the following:

- **Idle Key List:** Edit the field as described in the following example:

```
redial|1;newcall|2;dnd;psk1
```

If the user incorrectly configures the programmable softkey list features on the phone, the key list on the phone LCD does not update. For example:

- If a user enters **rdeial;newcall;cfwd** (redial has been misspelt), the key list is not updated and the user does not see any change on the LCD.
- If a user enters **redial;newcall;cfwd;delchar**, the user will not see a change on the LCD, as the delchar softkey is not allowed in the **Idle Key List**. Hence, this is an incorrect configuration of the programmable softkey list.

- **PSK1:**

```
fnc=sd;ext=5014@$PROXY;nme=sktest1
```

**Note** In this example, we are configuring a softkey on a phone as a speed dial number for extension 5014 (sktest1).

You can also configure an XML service on the programmable softkey. Enter the string in this format:

```
<PSK_1 ua="na">fnc=xml;url=http://xml.service.url;nme=name</PSK_1>
```

**Step 5** Click **Submit All Changes**.

## Configure a PSK with DTMF Support

You can configure programmable softkeys (PSK) with dual tone multifrequency (DTMF). This configuration enables the phone to send digital pulses inband (or out-of-band via SIP INFO) to the server during an active call. When you enable a function on a PSK, the user sees the softkey name, and presses it to perform the named function. The applied actions to the DTMF digit string are similar to those applied to Speed Dial, such as the following:

- **Pause** represented by ,
- **Wait** represented by X

For example, `ext=<DTMF_DIGITS>[[,|X][<DTMF_DIGITS>]]`, where the valid DTMF digits are 0-9,\*,#, a, b, c, d, and where the parts in [ ] brackets are optional.

This feature applies only to programmable softkeys. It doesn't apply to the programmable line keys (PLK) on the desk phones. If you configure any PLK for this feature, the display will present the Circled X icon (⊗), and nothing will happen if you press the key.

This feature supports only **Connected Key List** and **Connected Video Key List**.

**Before you begin**

[Access the Phone Web Interface, on page 100.](#)

**Procedure**

**Step 1** Select **Voice > Phone > Programmable Softkeys**.

**Step 2** Set the **Programmable Softkey Enable** field to **yes**.

**Step 3** From the PSK list (PSK#1 - PSK#16), select a PSK to configure.

**Step 4** In the **PSK(n)** field, where **n** is a programmable softkey number, enter a string in this format:

```
fnc=dtmf;ext=<dtmf_digits_to_be_outpulsed>;nme=<softkey_display_name>;
vid=<extension_n_to_be_associated>
```

When a phone has more than one registered line, you must include the **vid=** that is associated with the particular line/extension in order for the softkey to appear. Otherwise, the softkey will not display.

**Step 5** (Optional) To configure the PSK softkey to toggle within a pair (outpulse-display) each time you press it, enter a string in this format:

```
fnc=dtmf;ext=<dtmf_digits_to_be_outpulsed>;nme=<softkey_display_name>;
ext2=<second_set_of_dtmf_digits_to_be_outpulsed>;nme2=<second_softkey_display_name_after_first_press>;
vid=<extension_n_to_be_associated>
```

The PSK softkey toggle always starts with the **ext/nme** for each new call.

**Step 6** In the **Connected Key List** field or **Connected Video Key List** field, enter the configured PSK keywords according to where on the phone screen you wish the softkey name to appear.

For example, in the following entry, the **hold** softkey name appears in the first position. The softkey name that is listed in the **psk1** field appears in the second position, and so on.

```
hold;psk1;endcall;xfer;conf;xferLx;confLx;bxfer;phold;redial;dir;park
```

**Step 7** Select **Voice > Ext(n)**, where **n** is the extension number you wish to configure.

**Step 8** In the **Audio Configuration** section, set the **DTMF Tx Method** to one of the following methods from the drop-down list.

- InBand
- AVT
- INFO
- Auto
- InBand+INFO
- AVT+INFO

**Step 9** Click **Submit All Changes**.

Use these examples to help you understand how to configure PSK with DTMF Support options:

Example: PSK toggles when pressed.

- **Voice > Phone > Programmable Softkeys > Programmable Softkey Enable: Yes**

- **Connected Key List:** `psk1|1 ;endcall|2;conf|3;xfer|4;`
- **PSK 1:** `fnc=dtmf;ext=#1;nme=PressStart;ext2=*2;nme2=PressStop;vid=1`
- **Voice > Ext 1 > DTMF Tx Method:** `Auto`

Example: Phone sends DTMF digits inband via a PSK softkey.

- **Voice > Phone > Programmable Softkeys**
- **Programmable Softkey Enable:** `yes.`
- **Connected Key List:** `psk1|1;endcall|2;conf|3;xfer|4;`
- **PSK 1:** `fnc=dtmf;ext=#1;nme=PressMe;vid=1`
- **Voice > Ext 1 > DTMF Tx Method:** `Auto`

Example: The PSK softkey pauses between digits.

- **Voice > Phone > Programmable Softkeys > Programmable Softkey Enable:** `Yes`
- **Connected Key List:** `psk1|1;endcall|2;conf|3;xfer|4;`
- **PSK 1:** `fnc=dtmf;ext=#1,1006;nme=PressMe;vid=1`
- **Voice > Ext 1 > DTMF Tx Method:** `Auto`

Example: The PSK softkey waits for the user's input between digits.

- **Voice > Phone > Programmable Softkeys > Programmable Softkey Enable:** `Yes`
- **Connected Key List:** `psk1|1;endcall|2;conf|3;xfer|4;`
- **PSK 1:** `fnc=dtmf;ext=#1X1006;nme=PressMe;vid=1`
- **Voice > Ext 1 > DTMF Tx Method:** `Auto`

---

## Enable Softkeys to Calls History List Menu

You can configure the **Option**, **Call**, **Edit call**, **Filter**, and **Back** softkeys on the screen for All, Placed, Received, and Missed calls list. When you press the **Recents** softkey on the phone, you can directly access the **All calls** screen and see the list of all types of recents calls.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

---

- Step 1** Select **Voice > Phone**.

**Step 2** Configure the XSI account information by providing values in the **XSI Host Server**, **XSI Authentication Type**, **Login User ID**, **Login Password**, and **CallLog Associated Line** parameters.

For more information about configuring XSI account, see [Configure BroadSoft Settings, on page 311](#).

**Step 3** Set the **CallLog Enable** parameter to **Yes**.

**Step 4** Set **Display Recents From** to **Server**.

**Step 5** In the **Programmable Softkeys** section,

a. Set the **Programmable Softkey Enable** parameter to **Yes**.

b. In the **Broadsoft Call History Key List** field, the default string is: `option|1;call|2;editcall|3;back|4;`

Supported strings are `option`, `call`, `editcall`, `filter`, and `back`. This parameter doesn't support `psk` string.

Availability of all these softkeys under the All, Placed, Received, and Missed calls list or the **Option** menu in these calls list depends on the following conditions:

- **Programmable Softkey Enable = Yes** and **Broadsoft Call History Key List = `option|1;call|2;filter|3;back|4;`** - **Option**, **Call**, **Filter**, **Back** softkeys appear on the All, Placed, Received, and Missed calls list. **Edit call** appears in the **Option** menu of calls list.
- **Programmable Softkey Enable = Yes** and **Broadsoft Call History Key List = `option|1;call|2;back|4;`** - **Option**, **Call**, **Back** softkeys appear on the All, Placed, Received, and Missed calls list. **Edit call** and **Filter** appears in the **Option** menu of calls list.
- **Programmable Softkey Enable = Yes** and **Broadsoft Call History Key List = `option|1;call|2;editcall|3;filter|4;`** - **Option**, **Call**, **Edit call**, **Filter** softkeys appear on the All, Placed, Received, and Missed calls list.
- **Programmable Softkey Enable = Yes**, **PSK 1 = `fnc=shortcut;url=missedcalls`**, and **Broadsoft Call History Key List = `option|1;call|2;psk1|3;filter222|4;`** - only **Option** and **Call** softkeys appear on the All, Placed, Received, and Missed calls list because strings `psk` and `filter222` are invalid values. **Edit call** and **Filter** appears in the **Option** menu of calls list.
- **Programmable Softkey Enable = Yes**, and **Broadsoft Call History Key List = `blank`** - The softkeys appears as default setting `option|1;call|2;editcall|3`. **Option**, **Call**, **Edit call** softkeys appear on the All, Placed, Received, and Missed calls list. **Filter** appears in the **Option** menu of calls list.

**Note** In the phone configuration file with XML(cfg.xml), enter a string in this format:

```
<Broadsoft_Call_History_Key_List
ua="na">option|1;call|2;editcall|3</Broadsoft_Call_History_Key_List>
```

**Step 6** Click **Submit All Changes**.





## Spam Indication for Incoming Calls

New technology standard Secure Telephony Identity Revisited (STIR) and Signature-based Handling of Asserted information using toKENs (SHAKEN). These standards define procedures to authenticate and verify caller identification for calls carried over the IP network. The STIR-SHAKEN framework is developed to provide the end user with a great degree of identification and control over the type of calls they receive. These

sets of standards are intended to provide a basis for verifying calls, classifying calls, and facilitating the ability to trust caller identity end to end. Illegitimate callers can easily be identified.

When STIR/SHAKEN support is implemented on the server, the phone displays an extra icon next to the caller ID based on the caller's STIR/SHAKEN verification result. Based on the verification result, the phone displays three types of icons. This helps reduce wasted time from answering calls from robocallers, and the security risk from callers with spoofed or tampered Caller ID.



- Note**
- Validated call - When the caller carries `verstat=TN-Validation-Passed` in the SIP Header PAID or FROM, an extra icon  next to the caller id is displayed on the phone with a color screen indicating a validated caller. For a phone with grayscale screen, an extra icon  next to the caller id is displayed.
  - Spam call - When the caller carries `verstat=TN-Validation-Failed` in the SIP Header PAID or FROM, an extra icon  next to the caller id is displayed on the phone indicating an illegitimate caller.
  - Unverified call - When the caller carries `verstat=NO-TN-Validation` in the SIP Header PAID or FROM, an extra icon  next to the caller id is displayed on the phone indicating an unverified call.

For detailed spam notifications for calls in Webex environment, see [Spam Indication for Incoming Webex Calls](#), on page 270.

## Programmable Softkeys

| Keyword     | Key Label   | Definition   | Available Phone Status     |
|-------------|-------------|--|----------------------------|
| acd_login   | Agt signin  | Logs user in to Automatic Call Distribution (ACD).                                     | Idle                       |
| acd_logout  | AgtSignOut  | Logs user out of ACD.  | Idle                       |
| answer      | Answer      | Answers an incoming call.  | Ringing                    |
| astate      | Agt Status  | Checks the ACD status.   | Idle                       |
| avail       | Avail       | Denotes that a user who is logged in to an ACD server has set his status as available. | Idle                       |
| barge       | Barge       | Allows another user to interrupt a shared call.  | Shared-Active, Shared-Held |
| bargesilent | BargeSilent | Allows another user to interrupt a shared call with the mic disabled.                  | Shared-Active              |



| Keyword        | Key Label                   | Definition   | Available Phone Status  |
|----------------|-----------------------------|--|---|
| bxfer          | BlindXfer                   | Performs a blind call transfer (transfers a call without speaking to the party to whom the call is transferred). Requires that Blind Xfer Serv is enabled. | Connected<br>Connected Video  |
| call (or dial) | Call                        | Calls the selected item in a list.   | Dialing Input   |
| call info      | Call Info                   | Show call information  | Progressing   |
| calllist       | Call list                   | Provides access to the call list while on a connected video call.  | Connected, Connected Video  |
| cancel         | Cancel                      | Cancels a call (for example, when conferencing a call and the second party is not answering).  | Off-Hook  |
| cfwd           | Forward / Clr fwd           | Forwards all calls to a specified number.  | Idle, Off-Hook, Shared-Active, Hold, Shared-Held  |
| crdpause       | PauseRec                    | Pause recording  | Connected, Conferencing   |
| crdresume      | ResumeRec                   | Resume recording   | Connected, Conferencing   |
| crdstart       | Record                      | Start a recording  | Connected, Conferencing   |
| crdstop        | StopRec                     | Stop recording   | Connected, Conferencing   |
| conf           | Conference                  | Initiates a conference call. Requires that Conf Server is enabled and there are two or more calls that are active or on hold.                              | Connected<br>Connected Video  |
| confLx         | Conf line                   | Conferences active lines on the phone. Requires that Conf Serv is enabled and there are two or more calls that are active or on hold.                      | Connected<br>Connected Video  |
| delchar        | delChar -<br>backspace Icon | Deletes a character when entering text.  | Dialing Input   |
| dir            | Dir                         | Provides access to phone directories.  | Idle, Miss, Off-Hook (no input), Connected, Start-Xfer, Start-Conf, Conferencing, Hold, Ringing, Shared-Active, Shared-Held |
| disp_code      | DispCode                    | Enter Disposition Code   | Idle, Connected, Conferencing, Hold   |
| dnd            | DND / Clr Dnd               | Sets Do Not Disturb to prevent calls from ringing the phone.   | Idle, Off-Hook, Hold, Shared-Active, Shared-Held, Conferencing, Start-Conf, Start-Xfer, Connected video                     |

| Keyword                | Key Label       | Definition   | Available Phone Status   |
|------------------------|-----------------|--|--|
| emergency              | Emergency       | Enter emergency number   | Connected  |
| em_login (or signin)   | Sign in         | Logs user in to Extension Mobility.  | Idle   |
| em_logout (or signout) | Sign out        | Logs user out of Extension Mobility.   | Idle   |
| endcall                | End call        | Ends a call.   | Connected, Off-hook, Progressing, Start-Xfer, Start-Conf, Conferencing, Releasing, Hold, and Connected Video                                   |
| favorites              | Favorites       | Provides access to "Speed Dials".  | Idle, Miss, Off-Hook (no input), Connected, Start-Xfer, Start-Conf, Conferencing, Hold, Ringing, Shared-Active, Shared-Held<br>Connected Video |
| gpickup                | GrPickup        | Allows user to answer a call ringing on an extension by discovering the number of the ringing extension.   | Idle, Off-Hook   |
| hold                   | Hold            | Put a call on Hold.  | Connected, Start-Xfer, Start-Conf, Conferencing, Connected Video   |
| ignore                 | Decline         | Ignores an incoming call.  | Ringing  |
| ignoresilent           | Ignore          | Silences an incoming call  | Ringing  |
| join                   | Join            | Connects a conference call. If the conference host is user A and users B & C are participants, when A presses "Join", A will drop off and users B & C will be connected. | Conferencing   |
| lcr                    | Call Rtn/lcr    | Returns the last missed call.  | Idle, Missed-Call, Off-Hook (no input)   |
| left                   | Left arrow icon | Moves the cursor to the left.  | Dialing Input  |
| messages               | Messages        | Provides access to voicemail.  | Idle, Miss, Off-Hook (no input), Connected, Start-Xfer, Start-Conf, Conferencing, Hold, Ringing, Shared-Active, Shared-Held<br>Connected Video |

| Keyword   | Key Label             | Definition  | Available Phone Status  |
|-----------|-----------------------|---|---|
| miss      | Miss                  | Displays the list of missed calls.  | Missed-Call   |
| newcall   | New Call              | Begins a new call.  | Idle, Hold, Shared-Active, Shared-Held  |
| option    | Option                | Opens a menu of input options.  | Off-Hook  |
| park      | Park                  | Puts a call on hold at a designated "park" number.  | Connected<br>Connected Video  |
| phold     | PrivHold              | Puts a call on hold on an active shared line.   | Connected<br>Connected Video  |
| pickup    | PickUp                | Allows a user to answer a call ringing on another extension by entering the extension number.     | Idle, Off-Hook  |
| pip       | PIP icon              | Allows user to move PIP to one of the four corners of the screen or turn PIP off.                 | Connected Video   |
| recents   | Recents               | Displays the All calls list from call history.  | Idle, Off-Hook, Shared-Active, Shared-Held  |
| redial    | Redial                | Displays the redial list.   | Idle, Connected, Start-Conf, Start-Xfer, Off-Hook (no input), Hold<br>Connected Video |
| resume    | Resume                | Resumes a call that is on hold.   | Hold, Shared-Held   |
| right     | Right arrow icon      | Moves the cursor to the right.  | Dialing (input)   |
| settings  | Settings              | Provides access to "Information and Settings".  | All   |
| showvideo | Show video            | Provides access to the video session while on a connected video call and the call list is in view | Connected   |
| starcode  | Input Star Code/*code | Displays a list of star codes that can be selected.   | Off-Hook, Dialing (input)   |
| swap      | Swap                  | Allows user to swap the remote video stream and selfview during an active video call.             | Connected Video   |
| trace     | Trace                 | Trigger trace   | Idle, Connected, Conferencing, Hold   |

| <b>Keyword</b> | <b>Key Label</b> | <b>Definition</b>   | <b>Available Phone Status</b>                               |
|----------------|------------------|---|---|
| unavail        | Unavail          | Denotes that a user who is logged in to an ACD server has set his status as unavailable.  | Idle  |
| unpark         | Unpark           | Resumes a parked call.  | Idle, Off-Hook, Connected, Shared-Active<br>Connected Video |
| xfer           | Transfer         | Performs a call transfer. Requires that Attn Xfer Serv is enabled and there is at least one connected call and one idle call.                                 | Connected, Start-Xfer, Start-Conf                           |
| xferlx         | Xfer line        | Transfers an active line on the phone to a called number. Requires that Attn Xfer Serv is enabled and there are two or more calls that are active or on hold. | Connected<br>Connected Video                                |



## CHAPTER 13

# Audio Configuration

---

- [Configure Different Audio Volume](#) , on page 283
- [Configure the Voice Codecs](#), on page 284
- [Voice Quality Reporting](#), on page 289

## Configure Different Audio Volume

You can configure the volume settings in the phone web interface.

You can also configure the parameters in the phone configuration file with XML (cfg.xml) code. To configure each parameter, see the syntax of the string in the **Parameters for Audio Volume** table in [Parameters for Audio Volume](#), on page 283.

### Before you begin

[Access the Phone Web Interface](#), on page 100.

### Procedure

---

- Step 1** Select **Voice > User**.
  - Step 2** In the **Audio Volume** section, configure the volume level for audio parameters as described in the **Parameters for Audio Volume** table in [Parameters for Audio Volume](#), on page 283.
  - Step 3** Click **Submit All Changes**.
- 

## Parameters for Audio Volume

The following two tables describes the acoustic and audio settings.

The following table defines the function and usage of Audio Volume parameters in the Audio Volume section under the User tab in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file with XML(cfg.xml) code to configure a parameter.

**Table 43: Parameters for Audio Volume**

| Parameter      | Description   |
|----------------|---|
| Ringer Volume  | <p>Sets the default volume for the ringer.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:<br/> <pre>&lt;Ringer_Volume ua="rw"&gt;8&lt;/Ringer_Volume&gt;</pre> </li> <li>In the phone web page, enter a valid value as the ringer volume.</li> </ul> <p>Allowed values: an integer ranging between 0 and 15<br/>           Default: 9</p>            |
| Speaker Volume | <p>Sets the default volume for the speakerphone.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:<br/> <pre>&lt;Speaker_Volume ua="rw"&gt;11&lt;/Speaker_Volume&gt;</pre> </li> <li>In the phone web page, enter a valid value as the speaker volume.</li> </ul> <p>Allowed values: an integer ranging between 0 and 15<br/>           Default: 11</p> |
| Handset Volume | <p>Sets the default volume for the handset.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:<br/> <pre>&lt;Handset_Volume ua="rw"&gt;9&lt;/Handset_Volume&gt;</pre> </li> <li>In the phone web page, enter a valid value as the handset volume.</li> </ul> <p>Allowed values: an integer ranging between 0 and 15<br/>           Default: 10</p>       |

## Configure the Voice Codecs

A codec resource is considered allocated if it has been included in the SDP codec list of an active call, even though it eventually might not be chosen for the connection. Negotiation of the optimal voice codec sometimes depends on the ability of the Cisco IP Phone to match a codec name with the far-end device or gateway codec

name. The phone allows the network administrator to individually name the various codecs that are supported such that the correct codec successfully negotiates with the far-end equipment.

The Cisco IP Phone supports voice codec priority. You can select up to three preferred codecs. The administrator can select the low-bit-rate codec that is used for each line. G.711a and G.711u are always enabled.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code. To configure each parameter, see the syntax of the string in [Audio Codec Parameters, on page 285](#).

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

- 
- Step 1** Select **Voice > Ext(n)**, where n is an extension number.
- Step 2** In the **Audio Configuration** section, configure the parameters as defined in the [Audio Codec Parameters, on page 285](#) table.
- Step 3** Click **Submit All Changes**.
- 

## Audio Codec Parameters

The following table defines the function and usage of the voice codec parameters in the **Audio Configuration** section under the **Voice > Ext (n)** tab in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file (cfg.xml) with XML code to configure a parameter.

*Table 44: Audio Codec Parameters*

| Parameter       | Description  |
|-----------------|--|
| Preferred Codec | <p>Preferred codec for all calls. The actual codec used in a call still depends on the outcome of the codec negotiation protocol.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:<br/> <pre>&lt;Preferred_Codec_1_ua="rw"&gt;G711u&lt;/Preferred_Codec_1_&gt;</pre> </li> <li>In the phone web interface, select your preferred codec from the list.</li> </ul> <p>Allowed values: G711u G711a G729a G722 G722.2 iLBC OPUS</p> <p>Default: G711u</p> |

| Parameter              | Description   |
|------------------------|---|
| Use Pref Codec Only    | <p>Select <b>No</b> to use any code. Select <b>Yes</b> to use only the preferred codes. When you select Yes, calls fail if the far end does not support the preferred codecs.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:<br/> <pre>&lt;Use_Pref_Codec_Only_1_ ua="rw"&gt;No&lt;/Use_Pref_Codec_Only_1_&gt;</pre> </li> <li>In the phone web interface, set this field to Yes or No as needed.</li> </ul> <p>Allowed values: Yes No<br/> Default: No</p>    |
| Second Preferred Codec | <p>Codec to use if the codec specified in <b>Preferred Codec</b> fails.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:<br/> <pre>&lt;Second_Preferred_Codec_1_ ua="rw"&gt;Unspecified&lt;/Second_Preferred_Codec_1_&gt;</pre> </li> <li>In the phone web interface, select your preferred codec from the list.</li> </ul> <p>Allowed values: Unspecified G711u G711a G729a G722 G722.2 iLBC OPUS<br/> Default: Unspecified</p>                                 |
| Third Preferred Codec  | <p>Codec to use if the codecs specified in <b>Preferred Codec</b> and <b>Second Preferred Codec</b> fail.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:<br/> <pre>&lt;Third_Preferred_Codec_1_ ua="rw"&gt;Unspecified&lt;/Third_Preferred_Codec_1_&gt;</pre> </li> <li>In the phone web interface, select your preferred codec from the list.</li> </ul> <p>Allowed values: Unspecified G711u G711a G729a G722 G722.2 iLBC OPUS<br/> Default: Unspecified</p> |



| Parameter   | Description   |
|---|---|
| G711u Enable<br>G711a Enable<br>G729a Enable<br>G722 Enable<br>G722.2 Enable<br>iLBC Enable | <p>Enables the use of a specific codec.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:               <pre>&lt;G711u_Enable_1_ ua="rw"&gt;Yes&lt;/G711u_Enable_1_&gt;</pre> <pre>&lt;G711a_Enable_1_ ua="rw"&gt;Yes&lt;/G711a_Enable_1_&gt;</pre> <pre>&lt;G729a_Enable_1_ ua="rw"&gt;Yes&lt;/G729a_Enable_1_&gt;</pre> <pre>&lt;G722_Enable_1_ ua="rw"&gt;Yes&lt;/G722_Enable_1_&gt;</pre> <pre>&lt;G722_Enable_1_ ua="rw"&gt;Yes&lt;/G722_Enable_1_&gt;</pre> <pre>&lt;G722.2_Enable_1_ ua="rw"&gt;No&lt;/G722.2_Enable_1_&gt;</pre> <pre>&lt;iLBC_Enable_1_ ua="rw"&gt;No&lt;/iLBC_Enable_1_&gt;</pre> <pre>&lt;OPUS_Enable_1_ ua="rw"&gt;Yes&lt;/OPUS_Enable_1_&gt;</pre> </li> <li>In the phone web interface, set the corresponding field to <b>Yes</b> to enable the use of a specific codec, or <b>No</b> to disable it.</li> </ul> <p><b>Note</b> The transmit rate for the G.729a codec is at 8 kbps.</p> |
| Silence Supp Enable   | <p>Enables or disables silence suppression. When set <b>Yes</b>, silent audio frames are not transmitted.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:               <pre>&lt;Silence_Supp_Enable_1_ ua="rw"&gt;No&lt;/Silence_Supp_Enable_1_&gt;</pre> </li> <li>In the phone web interface, set this field to <b>Yes</b> to enable silence suppression, or <b>No</b> to disable it.</li> </ul> <p>Allowed values: Yes No</p> <p>Default: No</p>  |

| Parameter         | Description  |
|-------------------|--|
| DTMF Tx Method    | <p>The method for transmitting DTMF signals to the far end. The options are:</p> <ul style="list-style-type: none"> <li>• AVT—Audio video transport. Sends DTMF as AVT events.</li> <li>• InBand—Sends DTMF by using the audio path.</li> <li>• Auto—Uses InBand or AVT based on the outcome of codec negotiation.</li> <li>• INFO—Uses the SIP INFO method.</li> <li>• InBand+INFO—Uses both the audio path and the SIP INFO method.</li> <li>• AVT+INFO—Uses both the AVT and the SIP INFO method.</li> </ul> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>• In the phone configuration file with XML(cfg.xml), enter a string in this format:<br/> <pre>&lt;DTMF_Tx_Method_1_ ua="rw"&gt;Auto&lt;/DTMF_Tx_Method_1_&gt;</pre> </li> <li>• In the phone web interface, select your preferred transmitting method from the list.</li> </ul> <p>Default: Auto</p> |
| Codec Negotiation | <p>When set to <b>Default</b>, the phone responds to an Invite with a 200 OK response advertising the preferred codec only. When set to <b>List All</b>, the phone responds listing all the codecs that the phone supports.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>• In the phone configuration file with XML(cfg.xml), enter a string in this format:<br/> <pre>&lt;Codec_Negotiation_1_ ua="na"&gt;Default&lt;/Codec_Negotiation_1_&gt;</pre> </li> <li>• In the phone web interface, select the desired option from the list.</li> </ul> <p>Allowed values: Default List All</p> <p>Default: Default</p>   |
| Encryption Method | <p>Encryption method to be used during secured call. Options are AES 128 and AES 256 GCM</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>• In the phone configuration file with XML(cfg.xml), enter a string in this format:<br/> <pre>&lt;Encryption_Method_1_ ua="na"&gt;AES 128&lt;/Encryption_Method_1_&gt;</pre> </li> <li>• In the phone web interface, select your preferred encryption method from the list.</li> </ul> <p>Allowed values: AES 128  AES 256 GCM</p> <p>Default: AES 128.</p>   |

## Voice Quality Reporting

You can capture voice quality metrics for Voice over Internet Protocol (VoIP) sessions with a Session Initiation Protocol (SIP) event package. Voice call quality information derived from RTP and call information from SIP is conveyed from a User Agent (UA) in a session (reporter) to a third party (collector).

The Cisco IP phone uses User Datagram Protocol (UDP) to send a SIP PUBLISH message to a collector server.

## Supported Scenarios for Voice Quality Reporting

Currently, only the basic call scenario supports voice quality reporting. A basic call can be a peer to peer incoming or outgoing call. The phone supports periodic SIP publish message.

## Mean Opinion Scores and Codecs

The voice quality metrics use Mean Opinion Score (MOS) to rate the quality. A MOS rating of 1 is the lowest quality; a MOS rating of 5 is the highest quality. The following table gives a description of some of the codecs and MOS scores. The phone supports all codecs. For all codecs, the phone sends the SIP Publish message.

| Codec                   | Complexity and Description  | MOS  | Minimum Call Duration for Valid MOS Value |
|-------------------------|---|--|---|
| G.711 (A-law and u-law) | Very low complexity. Supports uncompressed 64 kbps digitized voice transmission at one to ten 5 ms voice frames-per-packet. This codec provides the highest voice quality and uses the most bandwidth of any of the available codecs. | A minimum value of 4.1 indicates good voice quality. | 10 seconds                                |
| G.729A                  | Low to medium complexity.   | A minimum value of 3.5 indicates good voice quality. | 30 seconds                                |
| G.729AB                 | Contains the same reduced complexity modifications present in the G.729A.   | A minimum value of 3.5 indicates good voice quality. | 30 seconds                                |

## Configure Voice Quality Reporting

You can generate a voice quality report for each extension on the phone. The parameters for the Voice Quality Metrics (VQM) SIP Publish Message help you to:

- Generate voice quality reports.
- Name your reports.
- Determine when your phone sends SIP Publish messages.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code. See [VQM SIP Publish Message Parameters, on page 290](#)

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

- 
- Step 1** Select **Voice > Ext(n)**, where (n) is the extension number.
- Step 2** In **SIP Settings**, enter a value for the **Voice Quality Report Address** parameter. You can enter either a domain name or an IP address.
- You can also add a port number along with the domain name or an IP address for this parameter. If you do not enter a port number, the value of the **SIP UDP Port** (5060) is used by default. If the collector server URL parameter is blank, a SIP PUBLISH message is not sent out.
- Step 3** Enter your report name for the **Voice Quality Report Group** parameter. Your report name can't begin with a hyphen (-), semicolon (;), or a space.
- Step 4** Enter an interval, in seconds, for the **Voice Quality Report Interval** parameter. Example: **20** for 20-second interval reporting.
- Step 5** Click **Submit All Changes**.
- 

## VQM SIP Publish Message Parameters

The following table defines the Voice Quality Metrics (VQM) SIP Publish Message parameters in the **Sip Settings** section under **Voice > Ext(n)** tab in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file (cfg.xml) with XML code to configure a parameter.

**Table 45: VQM SIP Publish Message Parameters**

| Parameter Name               | Description  |
|------------------------------|--|
| Voice Quality Report Address | <p>Allows you to enter one of the following options:</p> <ul style="list-style-type: none"> <li>• Domain Name</li> <li>• IP address</li> <li>• The SIP UDP port number along with the domain name</li> </ul> <p>In the phone XML configuration file (cfg.xml), enter a string in this format:</p> <pre>&lt;Voice_Quality_Report_Address_1_ua="na"&gt;fake_vq_collector&lt;/Voice_Quality_Report_Address_1_&gt;</pre> <p>Default parameter = empty (no report)</p> <p>Default SIP UDP Port = 5060</p> |

| Parameter Name                | Description  |
|-------------------------------|--|
| Voice Quality Report Group    | <p>Allows you to enter a voice quality report name.</p> <p>Your report name cannot begin with a:</p> <ul style="list-style-type: none"> <li>• hyphen (-)</li> <li>• semicolon (;)</li> <li>• space</li> </ul> <p>In the phone XML configuration file (cfg.xml), enter a string in this format:</p> <pre>&lt;Voice_Quality_Report_Group_1_ua="na"&gt;test-group-1&lt;/Voice_Quality_Report_Group_1_&gt;</pre> <p>Default parameter = empty (The report will use the canonical name in the form of <b>identifier@ipAddress</b>.)</p>   |
| Voice Quality Report Interval | <p>Allows you to determine when the phones send SIP Publish messages.</p> <p>If you have properly configured the <b>Voice Quality Report Address</b>, the SIP Publish messages can be sent:</p> <ul style="list-style-type: none"> <li>• When the call has ended or is placed on hold.</li> <li>• Periodically, when you enter an interval in seconds for this parameter. Example: <b>20</b> for 20-second intervals.</li> </ul> <p>In the phone XML configuration file (cfg.xml), enter a string in this format:</p> <pre>&lt;VQ_Report_Interval_1_ua="na"&gt;20&lt;/VQ_Report_Interval_1_&gt;</pre> <p>Default parameter = 0 (no periodic SIP Publish Message)</p> |





## CHAPTER 14

# Voicemail Configuration

---

- [Configure Voicemail, on page 293](#)

## Configure Voicemail

You can configure the internal or external phone number or URL for the voicemail system. If you use an external voicemail service, the number must include any digits required to dial out and any required area code.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

---

- Step 1** Select **Voice > Phone**.
- Step 2** In the **General** section, enter the **Voice Mail Number** that is a phone number or URL to check the voicemail. You can also configure this parameter in the configuration file (cfg.xml) by entering a string in this format:
- ```
<Voice_Mail_Number ua="na">123</Voice_Mail_Number>
```
- Default: Empty
- Step 3** Click **Submit All Changes**.  
The phone reboots.
- 

## Configure Voicemail for An Extension

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

## Procedure

- 
- Step 1** Select **Voice > Ext(n)**, where **(n)** is the number of an extension.
- Step 2** In the **Call Feature Settings** section, configure the parameters **Voice Mail Server**, **Voice Mail Subscribe Interval** (optional), and **Voice Mail Enable** as described in [Parameters for Voicemail Server, on page 294](#).
- Step 3** Click **Submit All Changes**.
- The phone reboots.
- 

## Parameters for Voicemail Server

The following table describes the **Call Feature Settings** for Voicemail.

*Table 46: Parameters for Voicemail*

Parameter	Description
Voice Mail Server	<p>Identifies the SpecVM server for the phone, generally the IP address, and port number of the VM server.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file (cfg.xml), enter a string in this format:           <pre>&lt;Voice_Mail_Server_1_ua="na"&gt;&lt;/Voice_Mail_Server_1_&gt;</pre> </li> <li>In the phone web page, enter the IP address of the voicemail server.</li> </ul> <p>Default: Empty</p>
Voice Mail Subscribe Interval	<p>The expiration time, in seconds, of a subscription to a voicemail server.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file (cfg.xml), enter a string in this format:           <pre>&lt;Voice_Mail_Subscribe_Interval_1_ua="na"&gt;86400&lt;/Voice_Mail_Subscribe_Interval_1_&gt;</pre> </li> <li>In the phone web page, enter an appropriate value.</li> </ul> <p>Allowed values: An integer from 0 through 86400</p> <p>If the value is set to 0, then the phone uses the default value instead.</p> <p>Default: 86400</p>



Parameter	Description
Voice Mail Enable	<p>Enables or disables the subscription to the voicemail server for the specific extension.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"><li>• In the phone configuration file (cfg.xml), enter a string in this format: <pre>&lt;Voice_Mail_Enable_1_ua="na"&gt;Yes&lt;/Voice_Mail_Enable_1_&gt;</pre></li><li>• In the phone web interface, set this field to <b>Yes</b> or <b>No</b> to enable or disable the function.</li></ul> <p>Allowed values: Yes and No</p> <p>Default: Yes</p>





## CHAPTER 15

# Corporate and Personal Directory Setup

---

- [Configure Directory Services, on page 297](#)
- [LDAP Configuration, on page 301](#)
- [Configure BroadSoft Settings, on page 311](#)
- [Set up Personal Directory, on page 322](#)
- [Enable Reverse Name Lookup, on page 323](#)

## Configure Directory Services

With the Directory Services, you control the display of the directories:

- Personal address book
- All enabled directories

Also, you control the directory browse mode and the maximum number of contacts displayed on the phone.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

---

- Step 1** Select **Voice > Phone**.
  - Step 2** In the **Directory Services**, set up the fields as described in [Parameters for Directory Services, on page 297](#).
  - Step 3** Click **Submit All Changes**.
- 

## Parameters for Directory Services

The following table defines the function and usage of the parameters in the **Directory Services** section under the **Voice > Phone** tab in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file (cfg.xml) with XML code to configure a parameter.

Table 47: Parameters for Directory Services

Parameter	Description
Personal Directory Enable	<p>Enables the personal address book directory for the phone user.</p> <p>Select <b>Yes</b> to enable the directory and select <b>No</b> to disable it.</p> <p>If you disable the directory:</p> <ul style="list-style-type: none"> <li>• users can't search contacts from their personal address book</li> <li>• users can't add a contact in their personal address book</li> </ul> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>• In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="976 856 1474 905">&lt;Personal_Directory_Enable ua="na"&gt;Yes&lt;/Personal_Directory_Enable&gt;</pre> </li> <li>• In the phone web interface, set this field to <b>Yes</b> to enable the personal address book directory.</li> </ul> <p>Valid values: Yes No</p> <p>Default: Yes</p>

Parameter	Description
Search All Enable	<p>Determines whether the phone user can search for contacts in the <code>All</code> directories.</p> <p>Select <b>Yes</b> to enable the search operation and select <b>No</b> to disable it.</p> <p>The <code>All</code> directories contain the following directories with the priority from highest to lowest:</p> <ol style="list-style-type: none"> <li>1. Personal address book</li> <li>2. BroadSoft directory</li> <li>3. LDAP directory</li> <li>4. Bluetooth phone directory</li> </ol> <p>The <code>All</code> directories only contain the enabled directories.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>• In the phone configuration file with XML(<code>cfg.xml</code>), enter a string in this format: <pre>&lt;Search_All_Enable ua="na"&gt;Yes&lt;/Search_All_Enable&gt;</pre> </li> <li>• In the phone web interface, set this field to <b>Yes</b> to enable the search operation.</li> </ul> <p>Valid values: Yes No Default: Yes</p>
Browse Mode Enable	<p>Determines whether to trigger an auto preload operation to show the contacts when you enter a directory in the phone.</p> <p>Select <b>Yes</b> to enable the browse mode for any directories and select <b>No</b> to disable it.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>• In the phone configuration file with XML(<code>cfg.xml</code>), enter a string in this format: <pre>&lt;Browse_Mode_Enable ua="na"&gt;Yes&lt;/Browse_Mode_Enable&gt;</pre> </li> <li>• In the phone web interface, set this field to <b>Yes</b> to enable the browse mode.</li> </ul> <p>Valid values: Yes No Default: No</p>

## Disable Contact Search in All Directories

By default, the user can search for contacts in all the directories on the phone. You can configure the phone to disable this feature. Then, the user can only search for a contact in a single directory each time.

When you complete this procedure, the **All directories** option doesn't display under the **Directories** menu on the phone screen.

You can also configure this parameter in the configuration file (cfg.xml) with a string in this format:

```
<Search_All_Enable ua="na">No</Search_All_Enable>
```

The valid values are Yes and No. The default setting is Yes.

### Procedure

---

- Step 1** Select **Voice > Phone**.
  - Step 2** In the **Directory Services** section, set the **Search All Enable** field to **No**.
  - Step 3** Click **Submit All Changes**.
- 

## Disable Personal Directory

By default, the personal directory is enabled on the phone. You can disable the personal directory from the phone web interface. When you disable the personal directory:

- the **Personal Directory** tab doesn't display in the phone web interface.
- the **Personal address book** option doesn't display on the **Directories** phone screen.
- the user can't add contacts to the personal directory from the call history or other directories.
- the phone skips the personal directory when the user searches for a contact in all the directories.
- as the user dials a number with the keypad or there is an incoming call, the phone skips the personal directory when it searches for a matching number in directories.

You can also configure the parameter in the configuration file (cfg.xml) with a string in this format:

```
<Personal_Directory_Enable ua="na">No</Personal_Directory_Enable>
```

The valid values are Yes and No. The default setting is Yes.

### Procedure

---

- Step 1** Select **Voice > Phone**.
  - Step 2** In the **Directory Services** section, set the **Personal Directory Enable** field to **No**.  
By default, this field is set to **Yes**.
  - Step 3** Click **Submit All Changes**.
-

# LDAP Configuration

The Cisco IP Phone supports Lightweight Directory Access Protocol (LDAP) v3. LDAP Corporate Directory Search allows a user to search a specified LDAP directory for a name, phone number, or both. LDAP-based directories, such as Microsoft Active Directory 2003 and OpenLDAP-based databases, are supported.

Users access LDAP from the **Directory** menu on their IP phone. An LDAP search returns up to 20 records.

The instructions in this section assume that you have installed an LDAP server, such as OpenLDAP or Microsoft Active Directory Server 2003.

## Prepare the LDAP Corporate Directory Search

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

- 
- Step 1** Select **Voice > System**.
- Step 2** In the **IPv4 Settings** section, enter the IP address of the DNS server in the **Primary DNS** field.
- This step is required only if you are using Active Directory with authentication set to MD5.
- You can configure this parameter in the configuration file by entering a string in this format:
- ```
<Primary_DNS ua="na">10.74.2.7</Primary_DNS>
```
- Step 3** In the **Optional Network Configuration** section, in the **Domain** field, enter the LDAP domain.
- This step is required only if you are using Active Directory with authentication set to MD5.
- Some sites might not deploy DNS internally and instead use Active Directory 2003. In this case, it is not necessary to enter a Primary DNS address and an LDAP Domain. However, with Active Directory 2003, the authentication method is restricted to Simple.
- You can configure this parameter in the configuration file by entering a string in this format:
- ```
<Domain ua="na">LDAPdomainname.com</Domain>
```
- Step 4** Click the **Phone** tab.
- Step 5** Configure the LDAP fields as described in [Parameters for LDAP Directory, on page 301](#).
- Step 6** Click **Submit All Changes**.
- 

## Parameters for LDAP Directory

The following table defines the function and usage of the LDAP directory parameters in the **LDAP** section under the **Voice > Phone** tab in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file (cfg.xml) with XML code to configure a parameter.

Table 48: Parameters for LDAP Directory

Parameter	Description
LDAP Dir Enable	<p>Enables or disables the LDAP directory.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <code>&lt;LDAP_Dir_Enable ua="na"&gt;Yes&lt;/LDAP_Dir_Enable&gt;</code></li> <li>In the phone web interface, set this field to <b>Yes</b> or <b>No</b> to enable or disable LDAP directory.</li> </ul> <p>Valid values: Yes and No  Default: No</p>
Corp Dir Name	<p>Enter a free-form text name, such as "Corporate Directory".</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <code>&lt;LDAP_Corp_Dir_Name ua="na"&gt;Coprporate Directory&lt;/LDAP_Corp_Dir_Name&gt;</code></li> <li>In the phone web interface, enter the name of the corporate directory.</li> </ul> <p>Valid values: Text string with no more than 63 characters  Default: Empty</p>
Server	<p>Enter a fully qualified domain name or IP address of an LDAP server.</p> <p>Enter the host name of the LDAP server if the MD5 authentication method is used.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <code>&lt;LDAP_Server ua="na"&gt;ldapserver.com&lt;/LDAP_Server&gt;</code></li> <li>In the phone web interface, enter IP address or host name of the LDAP server.</li> </ul> <p>Default: Empty</p>
Search Base	<p>Specify a starting point in the directory tree from which to search. Separate domain components [dc] with a comma. For example:  <code>dc=cv2bu,dc=com</code></p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <code>&lt;LDAP_Search_Base ua="na"&gt;dc=cv2bu,dc=com&lt;/LDAP_Search_Base&gt;</code></li> <li>In the phone web interface, enter the search base.</li> </ul> <p>Default: Empty</p>



Parameter	Description
Client DN	<p>Enter the distinguished name (DN) domain components [dc]; for example:  <code>dc=cv2bu,dc=com</code></p> <p>If you're using the default Active Directory schema (Name(cn)-&gt;Users-&gt;Domain), an example of the client DN follows:  <code>cn="David Lee",dc=users,dc=cv2bu,dc=com</code>  <code>cn="David Lee",dc=cv2bu,dc=com</code></p> <p><code>username@domain</code> is the client DN format for a Windows server</p> <p>For example, <code>DavidLee@cv2bu.com</code></p> <p>This parameter is available when <b>Auth Method</b> is set to <b>Simple</b>.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>• In the phone configuration file with XML(cfg.xml), enter a string in this format:  <code>&lt;LDAP_Client_DN ua="na"&gt;dc=cv2bu,dc=com&lt;/LDAP_Client_DN&gt;</code></li> <li>• In the phone web interface, enter the client domain name.</li> </ul> <p>Default: Empty</p>
User Name	<p>Enter the user name for a credentialed user on the LDAP server.</p> <p>This parameter is available when <b>Auth Method</b> is set to <b>DIGEST-MD5</b>.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>• In the phone configuration file with XML(cfg.xml), enter a string in this format:  <code>&lt;LDAP_User_Name ua="na"&gt;dc=cv2bu,dc=com&lt;/LDAP_User_Name&gt;</code></li> <li>• In the phone web interface, enter the user name.</li> </ul> <p>Default: Empty</p>
Password	<p>If you allow the user to access the LDAP directory without entering the credentials, enter the password for the user in this field. If you allow access of specific users, leave this field empty. The phone prompts for credentials to access the LDAP directory.</p> <p>User entry of credentials on the phone updates this field and the configuration file.</p> <p>The password entered in this field shows as the following in the configuration file (cfg.xml).</p> <pre>&lt;!-- &lt;LDAP_Password ua="na"&gt;*****&lt;/LDAP_Password &gt;--&gt;</pre> <p>Default: Empty</p>

Parameter	Description
Auth Method	<p>Select the authentication method that the LDAP server requires. Choices are:</p> <ul style="list-style-type: none"> <li>• None—No authentication is used between the client and the server.</li> <li>• Simple—The client sends its fully-qualified domain name and password to the LDAP server. Might present security issues.</li> </ul> <p>If selected, the phone prompts the <b>Client DN</b> and <b>Password</b> credentials to access the LDAP directory.</p> <p>If either or both of the credentials are empty, the operation used to authenticate the clients is the anonymous simple bind. The success of the operation depends on whether the LDAP server supports it.</p> <p>Users can access the LDAP directory without the need to enter the user credentials when the one of the following situations is satisfied:</p> <ul style="list-style-type: none"> <li>• The user credentials are cached on the phone.</li> <li>• The LDAP server allows the anonymous simple bind operation, and the operation succeeds. And the parameter <b>LDAP Prompt For Empty Credentials</b> is set to <b>No</b>.</li> </ul> <ul style="list-style-type: none"> <li>• Digest-MD5—The LDAP server sends authentication options and a token to the client. The client returns an encrypted response that is decrypted and verified by the server.</li> </ul> <p>If selected, the phone prompts the <b>Username</b> and <b>Password</b> credentials to access the LDAP directory.</p> <p>Users can access the LDAP directory without the need to enter the user credentials when the credentials are cached on the phone.</p> <p>For more information, see <a href="#">Overview of LDAP Directory Access, on page 310</a>.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>• In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;LDAP_Auth_Method ua="na"&gt;Simple&lt;/LDAP_Auth_Method&gt;</pre> </li> <li>• In the phone web interface, choose a authentication method.</li> </ul> <p>Default: None</p>

Parameter	Description
LDAP Prompt For Empty Credentials	<p>Enable or disable the LDAP sign-in prompt when there's no user credential on the phone. This function is used only for the simple authentication method that involves the anonymous simple bind operation.</p> <ul style="list-style-type: none"><li>• If the value is <b>Yes</b>, the phone always prompts for LDAP credentials. If the LDAP server supports the anonymous simple bind, users can either enter the credentials or leave them empty to access the LDAP directory.</li><li>• If the value is <b>No</b>, users can directly access the LDAP directory when the anonymous simple bind operation succeeds.</li></ul> <p>If the LDAP server doesn't support the anonymous simple bind (empty credentials), then the users must enter the client DN and password to access the LDAP directory.</p> <p>This parameter doesn't display on the phone administration web page. To configure the parameter, perform the following:</p> <p>In the phone configuration file with XML(cfg.xml), enter a string in this format:</p> <pre>&lt;LDAP_Prompt_For_Empty_Credentials ua="na"&gt;Yes&lt;/LDAP_Prompt_For_Empty_Credentials&gt;</pre> <p>Valid values: Yes and No</p> <p>Default: No</p>

Parameter	Description
StartTLS Enable	<p>Enable or disable the Start Transport Layer Security (StartTLS) operation. It provides the ability to establish TLS in an LDAP session.</p> <p>When <b>StartTLS Enable</b> is set to <b>Yes</b>, the phone behaviour vary depending on the LDAP server setting:</p> <ul style="list-style-type: none"> <li>• If the LDAP server is defined as “ldap://server:port”, then the phone sends the StartTLS request to the LDAP server.</li> <li>• If the LDAP server is defined as “ldaps://server:port”, then the phone directly performs the LDAP over TLS (LDAPS) operation.</li> </ul> <p>When <b>StartTLS Enable</b> is set to <b>No</b>, the phone behaviour vary depending on the LDAP server setting:</p> <ul style="list-style-type: none"> <li>• If the LDAP server is defined as “ldap://server:port”, then the phone performs the LDAP operation.</li> <li>• If the LDAP server is defined as “ldaps://server:port”, then the phone performs the LDAPS operation.</li> </ul> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>• In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;LDAP_StartTLS_Enable ua="na"&gt;Yes&lt;/LDAP_StartTLS_Enable&gt;</pre> </li> <li>• In the phone web interface, set this field to <b>Yes</b> or <b>No</b> to enable or disable the StartTLS operation.</li> </ul> <p>Valid values: Yes and No  Default: No</p>
Last Name Filter	<p>Use this field to specify how the phone must perform searches based on the last name or surname (sn), when users search for contacts.</p> <p>Examples:</p> <p><b>sn: (sn=\$VALUE*)</b> instructs the phone to find all last names that begin with the entered search string.</p> <p><b>sn: (sn=*\$VALUE*)</b> instructs the phone to find all last names in which the entered search string appears anywhere in the last name. This method is more inclusive and retrieves more search results. This method is consistent with the search method in other directories such as the BroadSoft directories and the user's personal address book on the phone.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>• In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;LDAP_Last_Name_Filter ua="na"&gt;sn:(sn=L*)&lt;/LDAP_Last_Name_Filter&gt;</pre> </li> <li>• In the phone web interface, enter the filter.</li> </ul> <p>Default: Empty</p>

Parameter	Description
First Name Filter	<p>Use this field to specify how the phone must perform searches based on the first name or common name (cn), when users search for contacts.</p> <p>Examples:</p> <p><b>cn : (cn=\$VALUE*)</b> instructs the phone to find all first names that begin with the entered search string.</p> <p><b>cn : (cn=*\$VALUE*)</b> instructs the phone to find all first names in which the entered search string appears anywhere in the first name. This method is more inclusive and retrieves more search results. This method is consistent with the search method in other directories such as the BroadSoft directories and the user's personal address book on the phone.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;LDAP_First_Name_Filter ua="na"&gt;cn: (cn=John*)&lt;/LDAP_First_Name_Filter&gt;</pre> </li> <li>In the phone web interface, enter the filter.</li> </ul> <p>Default: Empty</p>
Search Item 3	<p>Additional customized search item. Can be blank if not needed.</p> <p>This parameter is used only for the reserve name lookup feature for the LDAP directory. For more information about the feature, see <a href="#">Enable Reverse Name Lookup, on page 264</a>.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;LDAP_Search_Item_3 ua="na"&gt;search_item&lt;/LDAP_Search_Item_3&gt;</pre> </li> <li>In the phone web interface, enter a name for the additional item to search.</li> </ul> <p>Default: Empty</p>
Search Item 3 Filter	<p>Customized filter for the searched item. Can be blank if not needed.</p> <p>This parameter is used only for the reserve name lookup feature for the LDAP directory. For more information about the feature, see <a href="#">Enable Reverse Name Lookup, on page 264</a>.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;LDAP_Item_3_Filter ua="na"&gt;cn: (cn=John*)&lt;/LDAP_Item_3_Filter&gt;</pre> </li> <li>In the phone web interface, enter the filter.</li> </ul> <p>Default: Empty</p>

Parameter	Description
Search Item 4	<p>Additional customized search item. Can be blank if not needed.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;LDAP_Search_Item_4 ua="na"&gt;search_item&lt;/LDAP_Search_Item_4&gt;</pre> </li> <li>In the phone web interface, enter a name for the additional item to search.</li> </ul> <p>Default: Empty</p>
Search Item 4 Filter	<p>Customized filter for the searched item. Can be blank if not needed.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;LDAP_Item_4_Filter ua="na"&gt;cn:(cn=John*)&lt;/LDAP_Item_4_Filter&gt;</pre> </li> <li>In the phone web interface, enter the filter.</li> </ul> <p>Default: Empty</p>

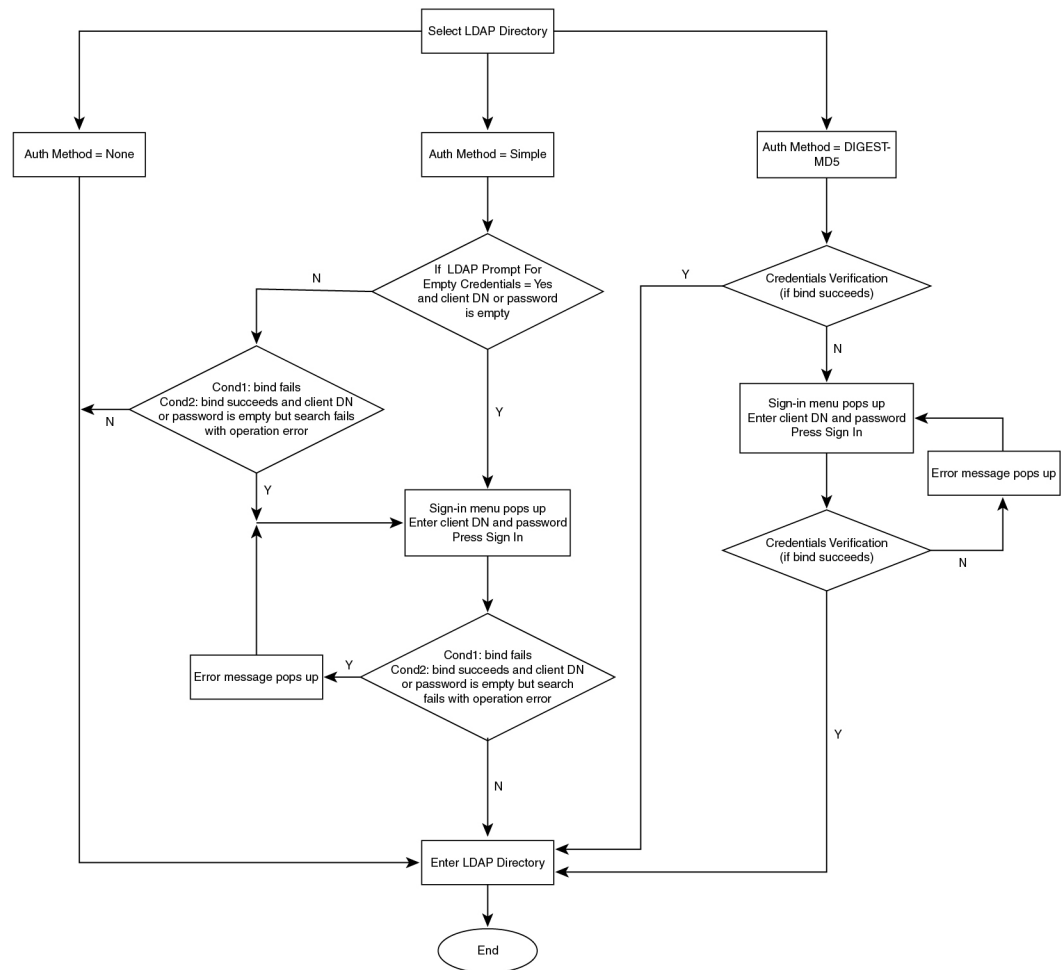
Parameter	Description
Display Attrs	<p>Format of LDAP results displayed on phone, where:</p> <ul style="list-style-type: none"> <li>• a—Attribute name For example, a=telephoneNumber means that the attribute name is used for a phone number. Other typical values: facsimileTelephoneNumber, mobile, mobiletelephonenumber, ipphone, homephone, otherphone, and pagertelephonenumber</li> <li>• cn—Common name</li> <li>• sn—Surname (last name)</li> <li>• n—Display name For example, n=Phone causes "Phone" to be displayed in front of the phone number of an LDAP query result when the details softkey is pressed.</li> <li>• t—type When t=p, that is, t is a phone number, the retrieved number can be dialed. Only one number can be made dialable. If two numbers are defined as dialable, only the first number is used. For example, a=ipPhone, t=p; a=mobile, t=p; This example results in only the IP Phone number being dialable and the mobile number is ignored.</li> <li>• p—phone number When p is assigned to a type attribute, example t=p, the retrieved number is dialable by the phone. For example, a=givenName,n=firstname;a=sn,n=lastname;a=cn,n=cn;a=telephoneNumber,n=tele,t=p</li> </ul> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>• In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;LDAP_Display_Attrs a=givenName,sn,telephoneNumber,ipphone,homephone,otherphone,pagertelephonenumber,cn,sn,n /&gt;</pre> </li> <li>• In the phone web interface, enter the attributes to display.</li> </ul> <p>Default: Empty</p>

Parameter	Description
Number Mapping	<p>With the LDAP number mapping, you can manipulate the number that was retrieved from the LDAP server. For example, you can append 9 to the number if your dial plan requires a user to enter 9 before dialing. Add the 9 prefix by adding (&lt;:9xx.&gt;) to the LDAP Number Mapping field. For example, 555 1212 would become 9555 1212.</p> <p>If you don't manipulate the number in this fashion, a user can use the <b>Edit Dial</b> feature to edit the number before dialing out.</p> <p>Leave this field blank if not needed.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>• In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;LDAP_Number_Mapping ua="na"&gt;&lt;:9xx.&gt;&lt;/LDAP_Number_Mapping&gt;</pre> </li> <li>• In the phone web interface, enter the mapping number.</li> </ul> <p>Default: Empty</p>

## Overview of LDAP Directory Access

The following diagram shows the logic of the LDAP directory access in different authentication methods:





450667

## Configure BroadSoft Settings

The BroadSoft directory service enables users to search and view their personal, group, or enterprise contacts. This application feature uses BroadSoft's Extended Services Interface (XSI).

To improve security, the phone firmware places access restrictions on the host server and directory name entry fields.

The phone uses two types of XSI authentication methods:

- User login credentials: The phone uses the XSI user id and password.
- SIP credentials: The register name and password of the SIP account registered on the phone. For this method, the phone can use the XSI user ID along with the SIP authentication credentials for the authentication.

## Procedure

- 
- Step 1** Select **Voice > Phone**.
- Step 2** In the **XSI Service** section, choose **Yes** from the **Directory Enable** drop down list box.
- You can also configure this parameter in the configuration file (cfg.xml) by entering a string in this format:
- ```
<Directory_Enable ua="na">Yes</Directory_Enable>
```
- Step 3** Set up the fields as described in [Parameters for XSI Phone Service, on page 312](#).
- Step 4** Click **Submit All Changes**.
- 

## Parameters for XSI Phone Service

The following table defines the function and usage of the XSI directory parameters in the **XSI Phone Service** section under the **Voice > Phone** tab in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file (cfg.xml) with XML code to configure a parameter.

*Table 49: Parameters for XSI Phone Service*

| Parameter       | Description   |
|-----------------|---|
| XSI Host Server | <p>Enter the name of the server; for example, <code>xsi.iopl.broadworks.net</code></p> <p><b>Note</b> XSI Host Server uses http protocol by default. To enable XSI over HTTPS, you can specify <code>https://</code> in the server.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;XSI_Host_Server ua="na"&gt;https://xsi.iopl.broadworks.net&lt;/XSI_Host_Server&gt;</pre> </li> <li>In the phone web interface, enter the XSI server to use.</li> </ul> <p>Default: Empty</p> |

| Parameter               | Description   |
|-------------------------|---|
| XSI Authentication Type | <p>Determines the XSI authentication type.</p> <p>Select <b>Login Credentials</b> to authenticate access with XSI id and password. Select <b>SIP Credentials</b> to authenticate access with the register user ID and password of the SIP account registered on the phone.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="1013 611 1487 659">&lt;XSI_Authentication_Type ua="na"&gt;SIP Credentials&lt;/XSI_Authentication_Type&gt;</pre> </li> <li>In the phone web interface, specify the authentication type for XSI service.</li> </ul> <p>Valid values: Login credentials SIP Credentials<br/>Default: Login Credentials</p>  |
| Login User ID           | <p>BroadSoft User ID of the phone user; for example, johndoe@xdp.broadsoft.com.</p> <p>Enter SIP Auth ID when you select <b>Login Credentials</b> or <b>SIP Credentials</b> for XSI authentication type.</p> <p>When you choose SIP Auth ID as <b>SIP Credentials</b>, you must enter Login User ID. Without Login User ID, the BroadSoft directory will not appear under the phone Directory list.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="1013 1310 1422 1358">&lt;Login_User_ID ua="na"&gt;username&lt;/Login_User_ID&gt;</pre> </li> <li>In the phone web interface, enter the username used to authenticate the access to the XSI server.</li> </ul> <p>Default: Empty</p> |
| Login Password          | <p>Alphanumeric password associated with the User ID.</p> <p>Enter login password, when you select <b>Login Credentials</b> for XSI authentication type.</p> <p>Default: Empty</p>  |

| Parameter        | Description  |
|------------------|--|
| SIP Auth ID      | <p>The registered user ID of the SIP account registered on the phone.</p> <p>Enter SIP Auth ID when you select <b>SIP Credentials</b> for XSI authentication type.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="976 579 1360 627">&lt;SIP_Auth_ID ua="na"&gt;username&lt;/SIP_Auth_ID&gt;</pre> </li> <li>In the phone web interface, enter the username used to authenticate the access to the XSI server.</li> </ul> <p>Default: Empty</p>    |
| SIP Password     | <p>The password of the SIP account registered on the phone.</p> <p>Enter SIP password when you select <b>SIP Credentials</b> for XSI authentication type.</p> <p>Default: Empty</p>  |
| Directory Enable | <p>Enables BroadSoft directory for the phone user.</p> <p>Select <b>Yes</b> to enable the directory and select <b>No</b> to disable it.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="976 1272 1360 1320">&lt;Directory_Enable ua="na"&gt;Yes&lt;/Directory_Enable&gt;</pre> </li> <li>In the phone web interface, set this field to <b>Yes</b> to enable the BroadSoft directory.</li> </ul> <p>Valid values: Yes and No</p> <p>Default: No</p> |

| Parameter                        | Description   |
|----------------------------------|---|
| Directory Individual Mode Enable | <p>Enables the individual mode for the BroadSoft directories. The parameter is valid only when <b>Directory Enable</b> is set to <b>Yes</b>.</p> <p>When this mode is enabled, the individual BroadSoft directories (such as, Enterprise, Group, Personal, and so on) display in the phone.</p> <p>When this mode is disabled, only the <b>BroadSoft directory</b> displays in the phone.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"><li>• In the phone configuration file with XML(cfg.xml), enter a string in this format:<br/><pre>&lt;XsiDir_Individual_Mode_Enable<br/>ua="na"&gt;Yes&lt;/XsiDir_Individual_Mode_Enable&gt;</pre></li><li>• In the phone web interface, set this field to <b>Yes</b> to enable the individual mode for the BroadSoft directories.</li></ul> <p>Valid values: Yes and No</p> <p>Default: No</p> |

| Parameter      | Description   |
|----------------|---|
| Directory Type | <p>Select the type of BroadSoft directory:</p> <ul style="list-style-type: none"> <li>• Enterprise: Allows users to search on last name, first name, user or group ID, phone number, extension, department, or email address.</li> <li>• Group: Allows users to search on last name, first name, user ID, phone number, extension, department, or email address.</li> <li>• Personal: Allows users to search on last name, first name, or telephone number.</li> <li>• Enterprise Common: Allows users to search on name or number.</li> <li>• Group Common: Allows users to search on name or number.</li> </ul> <p>This parameter is valid only when "Directory Enable" is set to <b>Yes</b> and "Directory Individual Mode Enable" is set to <b>No</b>.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>• In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="976 1073 1422 1121">&lt;Directory_Type ua="na"&gt;Enterprise&lt;/Directory_Type&gt;</pre> </li> <li>• In the phone web interface, specify the type of BroadSoft directory.</li> </ul> <p>Valid values: Enterprise, Group, Personal, Enterprise Common, and Group Common</p> <p>Default: Enterprise</p> |
| Directory Name | <p>Name of the directory. Displays on the phone as a directory choice.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>• In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="976 1581 1382 1629">&lt;Directory_Name ua="na"&gt;DirName&lt;/Directory_Name&gt;</pre> </li> <li>• In the phone web interface, enter the name of the BroadSoft directory to display on the phone.</li> </ul> <p>Default: Empty</p> <p>If the value is empty, the phone displays "BroadSoft directory".</p>   |

| Parameter                 | Description  |
|---------------------------|--|
| Directory Personal Enable | <p>Enables the BroadSoft personal directory for the phone user.</p> <p>Select <b>Yes</b> to enable the directory and select <b>No</b> to disable it.</p> <p>The parameter is valid only when both <b>Directory Enable</b> and <b>Directory Individual Mode Enable</b> are set to <b>Yes</b>.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>• In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="1015 688 1477 741">&lt;XsiDir_Personal_Enable ua="na"&gt;Yes&lt;/XsiDir_Personal_Enable&gt;</pre> </li> <li>• In the phone web interface, set this field to <b>Yes</b> to enable the directory.</li> </ul> <p>Valid values: Yes and No</p> <p>Default: No</p> |
| Directory Personal Name   | <p>Name of the BroadSoft personal directory. Displays on the phone as a directory choice.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>• In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="1015 1167 1528 1220">&lt;XsiDir_Personal_Name ua="na"&gt;DirPersonalName&lt;/XsiDir_Personal_Name&gt;</pre> </li> <li>• In the phone web interface, enter the name of the directory to display on the phone.</li> </ul> <p>Default: Empty</p> <p>If the value is empty, the phone displays “Personal”.</p>   |

| Parameter              | Description  |
|------------------------|--|
| Directory Group Enable | <p>Enables the BroadSoft group directory for the phone user.</p> <p>Select <b>Yes</b> to enable the directory and select <b>No</b> to disable it.</p> <p>The parameter is valid only when both <b>Directory Enable</b> and <b>Directory Individual Mode Enable</b> are set to <b>Yes</b>.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="976 688 1398 737">&lt;XsiDir_Group_Enable ua="na"&gt;Yes&lt;/XsiDir_Group_Enable&gt;</pre> </li> <li>In the phone web interface, set this field to <b>Yes</b> to enable the directory.</li> </ul> <p>Valid values: Yes and No</p> <p>Default: No</p> |
| Directory Group Name   | <p>Name of the BroadSoft group directory. Displays on the phone as a directory choice.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="976 1167 1485 1215">&lt;XsiDir_Group_Name ua="na"&gt;DirGroupName&lt;/XsiDir_Group_Name&gt;</pre> </li> <li>In the phone web interface, enter the name of the directory to display on the phone.</li> </ul> <p>Default: Empty</p> <p>If the value is empty, the phone displays “Group”.</p>   |



| Parameter                   | Description  |
|-----------------------------|--|
| Directory Enterprise Enable | <p>Enables the BroadSoft enterprise directory for the phone user.</p> <p>Select <b>Yes</b> to enable the directory and select <b>No</b> to disable it.</p> <p>The parameter is valid only when both <b>Directory Enable</b> and <b>Directory Individual Mode Enable</b> are set to <b>Yes</b>.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>• In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="1013 688 1500 737">&lt;XsiDir_Enterprise_Enable ua="na"&gt;Yes&lt;/XsiDir_Enterprise_Enable&gt;</pre> </li> <li>• In the phone web interface, set this field to <b>Yes</b> to enable the directory.</li> </ul> <p>Valid values: Yes and No</p> <p>Default: No</p> |
| Directory Enterprise Name   | <p>Name of the BroadSoft enterprise directory. Displays on the phone as a directory choice.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>• In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="1013 1167 1533 1215">&lt;XsiDir_Enterprise_Name ua="na"&gt;DirEnterpriseName&lt;/XsiDir_Enterprise_Name&gt;</pre> </li> <li>• In the phone web interface, enter the name of the directory to display on the phone.</li> </ul> <p>Default: Empty</p> <p>If the value is empty, the phone displays “Enterprise”.</p>   |

| Parameter                    | Description   |
|------------------------------|---|
| Directory GroupCommon Enable | <p>Enables the BroadSoft GroupCommon directory for the phone user.</p> <p>Select <b>Yes</b> to enable the directory and select <b>No</b> to disable it.</p> <p>The parameter is valid only when both <b>Directory Enable</b> and <b>Directory Individual Mode Enable</b> are set to <b>Yes</b>.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;XsiDir_GroupCommon_Enable ua="na"&gt;Yes&lt;/XsiDir_GroupCommon_Enable&gt;</pre> </li> <li>In the phone web interface, set this field to <b>Yes</b> to enable the directory.</li> </ul> <p>Valid values: Yes and No</p> <p>Default: No</p> |
| Directory GroupCommon Name   | <p>Name of the BroadSoft GroupCommon directory. Displays on the phone as a directory choice.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;XsiDir_GroupCommon_Name ua="na"&gt;DirGroupCommon&lt;/XsiDir_GroupCommon_Name&gt;</pre> </li> <li>In the phone web interface, enter the name of the directory to display on the phone.</li> </ul> <p>Default: Empty</p> <p>If the value is empty, the phone displays “Group Common”.</p>  |

| Parameter                         | Description  |
|-----------------------------------|--|
| Directory EnterpriseCommon Enable | <p>Enables the BroadSoft EnterpriseCommon directory for the phone user.</p> <p>Select <b>Yes</b> to enable the directory and select <b>No</b> to disable it.</p> <p>The parameter is valid only when both <b>Directory Enable</b> and <b>Directory Individual Mode Enable</b> are set to <b>Yes</b>.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="1015 688 1534 741">&lt;XsiDir_EnterpriseCommon_Enable ua="na"&gt;Yes&lt;/XsiDir_EnterpriseCommon_Enable&gt;</pre> </li> <li>In the phone web interface, set this field to <b>Yes</b> to enable the directory.</li> </ul> <p>Valid values: Yes and No</p> <p>Default: No</p> |
| Directory EnterpriseCommon Name   | <p>Name of the BroadSoft EnterpriseCommon directory. Displays on the phone as a directory choice.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="1015 1171 1534 1224">&lt;XsiDir_EnterpriseCommon_Name ua="na"&gt;DirEnterpriseCommon&lt;/XsiDir_EnterpriseCommon_Name&gt;</pre> </li> <li>In the phone web interface, enter the name of the directory to display on the phone.</li> </ul> <p>Default: Empty</p> <p>If the value is empty, the phone displays “Enterprise Common”.</p>  |

| Parameter                          | Description  |
|------------------------------------|--|
| Add Contacts to Directory Personal | <p>Enables the user to add contacts to the BroadSoft personal directory instead of the local personal address book.</p> <p>The parameter is valid only when <b>Directory Personal Enable</b> is set to <b>Yes</b>.</p> <ul style="list-style-type: none"> <li>If <b>Directory Personal Enable</b> is set to <b>No</b> and <b>Personal Directory Enable</b> is set to <b>Yes</b>, the contacts will be added to the local personal address book.</li> </ul> <p><b>Personal Directory Enable</b> is under the <b>Directory Services</b> section from <b>Voice &gt; Phone</b>.</p> <ul style="list-style-type: none"> <li>If both parameters are set to <b>No</b>, the user can't add the contacts on the phone.</li> </ul> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;Add_Contacts_to_Directory_Personal ua="na"&gt;Yes&lt;/Add_Contacts_to_Directory_Personal&gt;</pre> </li> <li>In the phone web interface, set this field to <b>Yes</b> to enable the feature.</li> </ul> <p>Valid values: Yes and No</p> <p>Default: No</p> |

## Set up Personal Directory

Phone users can set up personal directory from either the web interface or the **Contacts > Personal address book** menu on the phone. The setup of personal directory is not available in the configuration file (cfg.xml)

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

**Step 1** Select the **Personal Directory** tab.

**Step 2** You can do the following on this tab:

- Click **Add to Personal Directory** to add a contact to the personal address book.
  - Up to 3 phone numbers can be added to a contact entry.
- Click **Edit** on an existing contact entry to edit the contact information.

- Click **Assign** to assign a speed dial index to a phone number of the contact entry.
- Select an existing contact entry and click **Delete Contact** to delete it.

**Step 3** Click **Submit All Changes**.

---

## Enable Reverse Name Lookup

Reverse name lookup searches for the name of a number in an incoming, outgoing, conference, or transferred call. The reverse name lookup acts when the phone cannot find a name using the service provider directory, Call History, or your contacts. Reverse name lookup needs a valid BroadSoft (XSI) Directory, LDAP Directory, or XML Directory configuration.

The reverse name lookup searches the phone's external directories. When a search succeeds, the name is placed in the call session and in the call history. For simultaneous, multiple phone calls, reverse name lookup searches for a name to match the first call number. When the second call connects or is placed on hold, reverse name lookup searches for a name to match the second call. The reverse lookup searches the external directories for 8 secs, if in 8secs there are no results found, there will be no display of the name. If results are found in 8secs, the name is displayed on the phone. The external directory search priority order is : **BroadSoft (XSI) > LDAP > XML**.

While searching if the lower priority name is received before the higher priority name, the search shows the lower priority name first and then replaced it with the higher priority name if the higher priority name is found within 8 secs.

The precedence of the phone list lookup in BroadSoft (XSI) Directory is:

1. Personal phone list
2. Group common phone list
3. Enterprise common phone list

Reverse name lookup is enabled by default.

Reverse name lookup searches the directories in the following order:

1. Personal Address Book
2. SIP Header
3. Call History
4. BroadSoft (XSI) Directory
5. LDAP Directory
6. XML Directory



**Note** The phone searches the XML directory using this format: `directory_url?n=incoming_call_nu`  
Example: For a multiplatform phone using a third-party service, the phone number (1234) search quer this format, `http://your-service.com/dir.xml?n=1234`.

---

**Before you begin**

- Configure one of these directories before you can enable or disable the reverse name lookup:
  - BroadSoft (XSI) Directory
  - LDAP Corporate Directory
  - XML Directory
- Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

**Procedure**

---

**Step 1** Select **Voice > Phone**.

**Step 2** In the **Supplementary Services** area, set the **Reverse Phone Lookup Serv** parameter to **Yes** to enable this feature.

You can also configure this parameter in the configuration file (cfg.xml) by entering a string in this format:

```
<Reverse_Phone_Lookup_Serv ua="na">Yes</Reverse_Phone_Lookup_Serv>
```

The allowed values are Yes|No. The default value is Yes.

**Step 3** Click **Submit All Changes**.

---



PART **III**

# Cisco IP Phone Installation

- [Cisco IP Phone Installation, on page 327](#)







## CHAPTER 16

# Cisco IP Phone Installation

---

- [Verify the Network Setup, on page 327](#)
- [Install the Conference Phone \(8832\), on page 328](#)
- [Configure the Network from the Phone, on page 329](#)
- [Verify Phone Startup, on page 336](#)
- [Disable or Enable DF Bit, on page 336](#)
- [Configure Internet Connection Type, on page 337](#)
- [Configure VLAN Settings, on page 338](#)
- [SIP Configuration, on page 341](#)
- [NAT Transversal with Phones, on page 388](#)
- [Dial Plan, on page 397](#)
- [Regional Parameters Configuration, on page 404](#)
- [Cisco IP Conference Phone 8832 Multiplatform Phones Documentation, on page 421](#)

## Verify the Network Setup

For the phone to operate successfully as an endpoint in your network, your network must meet specific requirements.

### Procedure

---

- Step 1** Configure a VoIP Network to meet the following requirements:
- VoIP is configured on your routers and gateways.
- Step 2** Set up the network to support one of the following:
- DHCP support
  - Manual assignment of IP address, gateway, and subnet mask
-

# Install the Conference Phone (8832)

After the phone connects to the network, the phone startup process begins, and the phone registers with Third-party Call Control System. You need to configure the network settings on the phone if you disable the DHCP service.

After the phone connects, it determines if a new firmware load should be installed on the phone.

## Procedure

---

**Step 1** Choose the power source for the phone:

- Power over Ethernet (PoE) deployment with a Cisco IP Conference Phone 8832 PoE Injector
- Non-PoE Ethernet deployment with a Cisco IP Conference Phone 8832 Non-PoE Ethernet Injector

For more information, see [Ways to Provide Power to Your Conference Phone, on page 329](#).

**Step 2** Connect the phone to the switch.

- If you use PoE:
  - a. Plug the Ethernet cable into the LAN port.
  - b. Plug the other end of the Ethernet cable into either the Cisco IP Conference Phone 8832 PoE Injector or the Cisco IP Conference Phone 8832 Ethernet Injector.
  - c. Connect the injector to the conference phone with the USB-C cable.
- If you do not use PoE:
  - a. Connect the power adapter to the Cisco IP Conference Phone 8832 Ethernet Injector using a USB-C cable.
  - b. If you are using the Cisco IP Conference Phone 8832 Ethernet Injector, plug the power adapter into an electrical outlet.
  - c. Connect the power adapter to the Ethernet injector using a USB-C cable.

OR

If you are using the Cisco IP Conference Phone 8832 Non-PoE Ethernet Injector, plug it into an electrical outlet.

  - d. Plug the Ethernet cable into the Ethernet injector.
  - e. Plug the Ethernet cable into the Non-PoE Ethernet injector or the Ethernet injector.
  - f. Plug the Ethernet cable into the LAN port.
  - g. Connect the Ethernet injector to the conference phone using a second USB-C cable.
  - h. Connect the Non-PoE Ethernet injector or the Ethernet injector to the conference phone using a USB-C cable.

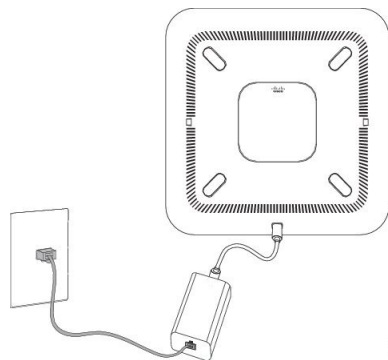
- Step 3** Monitor the phone startup process. This step verifies that the phone is configured properly.
- Step 4** If you do not use autoregistration, manually configure the security settings on the phone.
- Step 5** Allow the phone to upgrade to the current firmware image.
- Step 6** Make calls with the phone to verify that the phone and features work correctly.
- Step 7** Provide information to the users about how to use their phones and how to configure their phone options. This step ensures that users have adequate information to successfully use their Cisco conference phones.

## Ways to Provide Power to Your Conference Phone

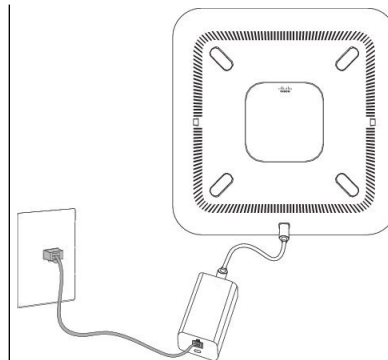
Your conference phone needs power from one of these sources:

- Power over Ethernet (PoE)
  - North America
    - Cisco IP Conference Phone 8832 PoE Injector
    - Cisco IP Conference Phone 8832 Ethernet Injector
  - Outside of North America—Cisco IP Conference Phone 8832 PoE Injector

**Figure 7: Conference Phone PoE Power Options**



Cisco IP Conference Phone 8832 PoE Injector with the PoE power option



Cisco IP Conference Phone 8832 Ethernet Injector with the PoE power option

## Configure the Network from the Phone

The phone includes many configurable network settings that you may need to modify before it is functional for your users. You can access these settings through the phone menus.

The Network configuration menu provides you with options to view and configure a variety of network settings.

You can configure settings that are display-only on the phone in your Third-Party Call Control system.

## Procedure

- 
- Step 1** Press **Settings**.
- Step 2** Select **Network configuration**.
- Step 3** Use the navigation arrows to select the desired menu and edit.
- Step 4** To display a submenu, repeat step 3.
- Step 5** To exit a menu, press **Back**.
- 

## Network Configuration Fields

Table 50: Network Configurations Menu Options

| Field                  | Field Type or Choices               | Default      | Description   |
|------------------------|-------------------------------------|--------------|---|
| Ethernet configuration |                                     |              | See the following Ethernet configuration submenu table.   |
| IP mode                | Dual mode<br>IPv4 only<br>IPv6 only | Dual mode    | Select the Internet Protocol mode for which the phone operates.<br>In dual mode, the phone can have both IPv4 and IPv6 addresses. |
| IPv4 address settings  | DHCP<br>Static IP                   | DHCP         | See the IPv4 address submenu table in the following tables.   |
| IPv6 address settings  | DHCP<br>Static IP                   | DHCP         | See the IPv6 address submenu table in the following tables.   |
| DHCPv6 option to use   |                                     | 17, 160, 159 | Indicates the order in which the phone uses the IPv6 addresses provided by DHCP server.   |
| HTTP proxy settings    |                                     |              | See the following HTTP proxy settings submenu table.  |
| Web server             | On<br>Off                           | On           | Indicates whether the phone has web server enabled or disabled.   |

Table 51: Ethernet Configuration Submenu

| Field                 | Field Type or Choices   | Default  | Description  |
|-----------------------|---|----------|--|
| 802.1x authentication | Device authentication   | Off      | Enables you to turn on or turn off the 802.1x authentication. Valid options are: <ul style="list-style-type: none"> <li>• On</li> <li>• Off</li> </ul>   |
|                       | Transaction status  | Disabled | <ul style="list-style-type: none"> <li>• Transaction status—Indicates different authentication status when you turn on 802.1x in the <b>Device authentication</b> field. <ul style="list-style-type: none"> <li>• Disabled—Default status.</li> <li>• Connecting—802.1x authentication started in the device.</li> <li>• Authenticated—802.1x authentication established in the device.</li> </ul> </li> <li>• Protocol—Specifies the protocol of the server.</li> </ul> |
| Switch port config    | Auto<br>10MB half<br>10MB full<br>100MB half<br>100MB full<br>1000 full | Auto     | Select speed and duplex of the network port.<br><br>If the phone is connected to a switch, configure the port on the switch to the same speed/duplex as the phone, or configure both to autonegotiate.<br><br>If you change the setting of this option, you must change the PC Port config option to the same setting.   |
| CDP                   | On<br>Off   | On       | Enable or disable Cisco Discovery Protocol (CDP).<br><br>CDP is a device-discovery protocol that runs on all Cisco manufactured equipment.<br><br>Using CDP, a device can advertise its existence to other devices and receive information about other devices in the network.   |
| LLDP-MED              | On<br>Off   | On       | Enable or disable LLDP-MED.<br><br>LLDP-MED enables the phone to advertise itself to devices that use the discovery protocol.  |

| Field            | Field Type or Choices | Default   | Description   |
|------------------|-----------------------|-----------|---|
| Startup delay    |                       | 3 seconds | Set a value that causes a delay for the switch to get to the forwarding state before the phone sends out the first LLDP-MED packet. For configuration of some switches, you might need to increase this value to a higher value for LLDP-MED to work. Configuring a delay can be important for networks that use the Spanning Tree Protocol.<br><br>Default delay is 3 seconds.   |
| VLAN             | On<br>Off             | Off       | Enable or disable VLAN.<br><br>Permits you to enter a VLAN ID when you use VLAN without CDP or LLDP. When you use a VLAN with CDP or LLDP, that associated VLAN takes precedent over the VLAN ID you manually entered.  |
| VLAN ID          |                       | 1         | Enter a VLAN ID for the IP phone when you use a VLAN without CDP (VLAN enabled and CDP disabled). Note that only voice packets are tagged with the VLAN ID. Do not use the 1 value for the VLAN ID. If VLAN ID is 1, you cannot tag voice packets with the VLAN ID.   |
| DHCP VLAN option |                       |           | Enter a predefined DHCP VLAN option to learn the voice VLAN ID.<br><br>When you use a VLAN ID with CDP, LLDP, or manually select a VLAN ID, that VLAN ID takes precedent over the selected DHCP VLAN option.<br><br>Valid values are: <ul style="list-style-type: none"> <li>• Null</li> <li>• 128 to 149</li> <li>• 151 to 158</li> <li>• 161 to 254</li> </ul> Default value is null.<br><br>Cisco recommends that you use DHCP Option 132. |

Table 52: IPv4 Address Settings Submenu

| Field           | Field Type or Choices | Default | Description  |
|-----------------|-----------------------|---------|--|
| Connection type | DHCP                  |         | <p>Indicates whether the phone has DHCP enabled.</p> <ul style="list-style-type: none"> <li>• DNS1—Identifies the primary Domain Name System (DNS) server that the phone uses.</li> <li>• DNS2—Identifies the secondary Domain Name System (DNS) server that the phone uses.</li> <li>• DHCP address released—Releases the IP address that DHCP assigned. You can edit this field if DHCP is enabled. To remove the phone from the VLAN and release the IP address for reassignment, set this field to Yes and press <b>Set</b>.</li> </ul>  |
|                 | Static IP             |         | <p>When DHCP is disabled, you must set the Internet Protocol (IP) address of the phone.</p> <ul style="list-style-type: none"> <li>• Static IP address—Identifies the IP that you assign to the phone. The phone uses this IP address instead of acquiring an IP from the DHCP server on the network.</li> <li>• Subnet Mask—Identifies the subnet mask used by the phone. When DHCP is disabled, you must set the subnet mask.</li> <li>• Gateway address—Identifies the default router used by the phone.</li> <li>• DNS1—Identifies the primary Domain Name System (DNS) server that the phone uses. When DHCP is disabled, you must set this field manually.</li> <li>• DNS2—Identifies the primary Domain Name System (DNS) server that the phone uses. When DHCP is disabled, you must set this field manually.</li> </ul> <p>When you assign an IP address using this field, you must also assign a subnet mask and a gateway address. See the Subnet Mask and Default Router fields in this table.</p> |

Table 53: IPv6 Address Settings Submenu

| Field           | Field Type or Choices | Default | Description  |
|-----------------|-----------------------|---------|--|
| Connection type | DHCP                  |         | <p>Indicates whether the phone has Dynamic Host Configuration Protocol (DHCP) enabled.</p> <ul style="list-style-type: none"> <li>• DNS1—Identifies the primary DNS server that the phone uses.</li> <li>• DNS2—Identifies the secondary DNS server that the phone uses.</li> <li>• Broadcast Echo—Identifies if the phone responds to multicast ICMPv6 message with destination address of ff02::1.</li> <li>• Auto config— Identifies if the phone uses automatic configuration for the address.</li> </ul>  |
|                 | Static IP             |         | <p>When DHCP is disabled, you must set the Internet Protocol (IP) address of the phone and must set the values of the fields:</p> <ul style="list-style-type: none"> <li>• Static IP—Identifies the IP that you assign to the phone. The phone uses this IP address instead of acquiring an IP from the DHCP server on the network.</li> <li>• Prefix length—Identifies how many bits of a Global Unicast IPv6 Address are there in the network part.</li> <li>• Gateway—Identifies the default router used by the phone.</li> <li>• Primary DNS—Identifies the primary DNS server that the phone uses. When DHCP is disabled, you must set this field manually.</li> <li>• Secondary DNS—Identifies the primary DNS server that the phone uses. When DHCP is disabled, you must set this field manually.</li> <li>• Broadcast Echo—Identifies if the phone responds to multicast ICMPv6 message with destination address of ff02::1.</li> </ul> |




Table 54: HTTP Proxy Settings Submenu

| Field      | Field Type or Choices | Description  |
|------------|-----------------------|--|
| Proxy mode | Auto                  | <p>Auto discovery (WPAD)—Enables or disables the Web Proxy Auto-Discovery protocol to retrieve a Proxy Auto-Configuration (PAC) file. Valid options are:</p> <ul style="list-style-type: none"> <li>• On</li> <li>• Off</li> </ul> <p>If the value is set to Off, you need to further set the following field:</p> <ul style="list-style-type: none"> <li>• PAC URL—Specifies the URL address for the PAC file that you want to retrieve. For example:</li> </ul> <pre>http://proxy.department.branch.example.com</pre> <p>The default value of Auto discovery (WPAD) is On.</p>   |
|            | Manual                | <ul style="list-style-type: none"> <li>• Proxy host—Specifies an IP address or hostname of the proxy server for the phone. The scheme (<code>http://</code> or <code>https://</code>) is not required.</li> <li>• Proxy port—Specifies a port number of the proxy server.</li> <li>• Proxy authentication—Selects an option according to the actual situation of the proxy server. If the server requires authentication credentials to grant access to the phone, then select On. Otherwise, select Off. Options are: <ul style="list-style-type: none"> <li>• Off</li> <li>• On</li> </ul> </li> </ul> <p>If the value is set to On, you need to further set the following fields:</p> <ul style="list-style-type: none"> <li>• Username—Specifies the username of a credential user on the proxy server.</li> <li>• Password—Provides the specified user's password to pass the authentication of the proxy server.</li> </ul> <p>The default value of Proxy authentication is Off.</p> |
|            | Off                   | Disables the HTTP proxy feature on the phone.  |

## Text and Menu Entry From the Phone

When you edit the value of an option setting, follow these guidelines:

- Use the arrows on the navigation pad to highlight the field that you wish to edit. Press **Select** in the navigation pad to activate the field. After the field is activated, you can enter values.
- Use the keys on the keypad to enter numbers and letters.

- To enter letters by using the keypad, use a corresponding number key. Press the key one or more times to display a particular letter. For example, press the **2** key once for “a,” twice quickly for “b,” and three times quickly for “c.” After you pause, the cursor automatically advances to allow you to enter the next letter.
- Press the softkey  if you make a mistake. This softkey deletes the character to the left of the cursor.
- Press **Back** before pressing **Set** to discard any changes that you made.
- To enter a period (for example, in an IP address), press \* on the keypad.



---

**Note** The Cisco IP Phone provides several methods to reset or restore option settings, if necessary.

---

## Verify Phone Startup

After the Cisco IP Phone has power connected to it, the phone automatically cycles through a startup diagnostic process.

### Procedure

---

- Step 1** If you are using Power over Ethernet, plug the LAN cable into the Network port.
- Step 2** If you are using the power cube, connect the cube to the phone and plug the cube into an electrical outlet.
- The buttons flash amber and then green in sequence during the various stages of bootup as the phone checks the hardware.
- If the phone completes these stages successfully, it has started up properly.
- 

## Disable or Enable DF Bit

You can disable or enable Don't Fragment (DF) bit in the TCP, UDP, or ICMP messages to determine whether a packet is allowed to be fragmented.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

---

- Step 1** Select **Voice > System**.
- Step 2** In the **Network Settings** section, configure the parameter **Disable DF**.

- If you set the **Disable DF** to **Yes**, the Don't Fragment (DF) bit is disabled. In this case, the network can fragment an IP packet. This is the default behaviour.
- If you set the **Disable DF** to **No**, the Don't Fragment (DF) bit is enabled. In this case, the network can't fragment an IP packet. This setting doesn't allow fragmentation in cases where the receiving host doesn't have sufficient resources to reassemble internet fragments.

**Step 3** Click **Submit All Changes**.

You can also configure the parameter in the phone configuration file (cfg.xml) with the following XML string:

```
<Disable_DF ua="na">Yes</Disable_DF>
```

Allowed values: Yes and No

Default: Yes

---

## Configure Internet Connection Type

You can choose how your phone receives an IP address. Set the connection type to one of the following:

- Static IP—A static IP address for the phone.
- Dynamic Host Configuration Protocol (DHCP)—Enables the phone to receive an IP address from the network DHCP server.

The Cisco IP phone typically operates in a network where a DHCP server assigns IP addresses to devices. Because IP addresses are a limited resource, the DHCP server periodically renews the phone lease on the IP address. If a phone loses the IP address, or if the IP address is assigned to another device on the network, the following occurs:

- Communication between the SIP proxy and the phone is severed or degraded.

The DHCP Timeout on Renewal parameter causes the phone to request renewal of its IP address if the following occurs:

- The phone doesn't receive an expected SIP response within programmable length of time after it sends a SIP command.

If the DHCP server returns the IP address that it originally assigned to the phone, the DHCP assignment is presumed to be operating correctly. Otherwise, the phone resets to try to fix the issue.

### Before you begin

[Access the Phone Web Interface, on page 100.](#)

### Procedure

---

**Step 1** Select **Voice > System**.

**Step 2** In the **IPv4 Settings** section, use the **Connection Type** drop-down list to choose the connection type:

- Dynamic Host Configuration Protocol (DHCP)
- Static IP

**Step 3** In the **IPv6 Settings** section, use the **Connection Type** drop-down list to choose the connection type:

- Dynamic Host Configuration Protocol (DHCP)
- Static IP

**Step 4** If you choose Static IP, configure these settings in the **Static IP Settings** section:

- **Static IP**—Static IP address of the phone
- **NetMask**—Netmask of the phone (IPv4, only)
- **Gateway**—Gateway IP address

**Step 5** Click **Submit All Changes**.

In the phone configuration XML file (cfg.xml), enter a string in this format:

```
<Connection_Type ua="rw">DHCP</Connection_Type>
<!-- available options: DHCP|Static IP -->
<Static_IP ua="rw"/>
<NetMask ua="rw"/>
<Gateway ua="rw"/>
```

## Configure VLAN Settings

The software tags your phone voice packets with the VLAN ID when you use a virtual LAN (VLAN).

In the VLAN Settings section of the **Voice > System** window, you can configure the different settings:

- LLDP-MED
- Cisco Discovery Protocol (CDP)
- Network Startup Delay
- VLAN ID (manual)
- DHCP VLAN Option

The multiplatform phones support these four methods to obtain VLAN ID information. The phone attempts to obtain the VLAN ID information in this order:

1. LLDP-MED
2. Cisco Discovery Protocol (CDP)
3. VLAN ID (manual)
4. DHCP VLAN Option

**Before you begin**

- Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).
- Disable CDP/LLDP and manual VLAN.

**Procedure**

- Step 1** Select **Voice > System**.
- Step 2** In the **VLAN Settings** section, configure the parameters as defined in the [VLAN Settings Parameters, on page 339](#) table.
- Step 3** Click **Submit All Changes**.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code. To configure each parameter, see the syntax of the string in the [VLAN Settings Parameters, on page 339](#) table.

## VLAN Settings Parameters

The following table defines the function and usage of each parameter in the **VLAN Settings Parameters** section under the **System** tab in the phone web page. It also defines the syntax of the string that is added in the phone configuration file with XML(cfg.xml) code to configure a parameter.

| Parameter Name | Description and Default Value  |
|----------------|--|
| Enable VLAN    | <p>Controls the VLAN feature.</p> <ul style="list-style-type: none"> <li>• In the phone configuration file with XML(cfg.xml), enter a string in this format:<br/> <pre>&lt;Enable_VLAN ua="rw"&gt;No&lt;/Enable_VLAN&gt;</pre> </li> <li>• In the phone web interface, set to <b>Yes</b> to enable VLAN.</li> </ul> <p>The default value is <b>Yes</b>.</p>  |
| VLAN ID        | <p>If you use a VLAN without CDP (VLAN enabled and CDP disabled), enter a VLAN ID for the IP phone. Note that only voice packets are tagged with the VLAN ID. Do not use 1 for the VLAN ID.</p> <ul style="list-style-type: none"> <li>• In the phone configuration file with XML(cfg.xml), enter a string in this format:<br/> <pre>&lt;VLAN_ID ua="rw"&gt;1&lt;/VLAN_ID&gt;</pre> </li> <li>• In the phone web interface, enter an appropriate value.</li> </ul> <p>Valid values: An integer ranging from 0 through 4095<br/> Default: 1</p> |

| Parameter Name  | Description and Default Value  |
|-----------------|--|
| PC Port VLAN ID | <p>Allows you to enter a VLAN ID for the PC port.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="976 426 1321 478">&lt;PC_Port_VLAN_ID ua="na"&gt;1&lt;/PC_Port_VLAN_ID&gt;</pre> </li> <li>In the phone web interface, enter an appropriate value.</li> </ul> <p>Valid values: An integer ranging from 0 through 4095<br/>Default: 1</p>  |
| Enable CDP      | <p>Enable CDP only if you are using a switch that has Cisco Discovery Protocol. CDP is negotiation based and determines which VLAN the IP phone resides in.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="976 884 1435 905">&lt;Enable_CDP ua="na"&gt;Yes&lt;/Enable_CDP&gt;</pre> </li> <li>In the phone web page: set to <b>Yes</b> to enable CDP.</li> </ul> <p>Valid values: Yes/No<br/>Default: Yes</p>  |
| Enable LLDP-MED | <p>Choose <b>Yes</b> to enable LLDP-MED for the phone to advertise itself to devices that use that discovery protocol.</p> <p>When the LLDP-MED feature is enabled, after the phone has initialized and Layer 2 connectivity is established, the phone sends out LLDP-MED PDU frames. If the phone receives no acknowledgment, the manually configured VLAN or default VLAN will be used if applicable. If the CDP is used concurrently, the waiting period of 6 seconds is used. The waiting period will increase the overall startup time for the phone.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="976 1583 1344 1635">&lt;Enable_LLDP-MED ua="na"&gt;Yes&lt;/Enable_LLDP-MED&gt;</pre> </li> <li>In the phone web interface, set to <b>Yes</b> to enable LLDP-MED.</li> </ul> <p>Valid values: Yes/No<br/>Default: Yes</p> |

| Parameter Name        | Description and Default Value   |
|-----------------------|---|
| Network Startup Delay | <p>Setting this value causes a delay for the switch to get to the forwarding state before the phone will send out the first LLDP-MED packet. The default delay is 3 seconds. For configuration of some switches, you might need to increase this value to a higher value for LLDP-MED to work. Configuring a delay can be important for networks that use Spanning Tree Protocol.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="1015 646 1437 703">&lt;Network_Startup_Delay ua="na"&gt;3&lt;/Network_Startup_Delay&gt;</pre> </li> <li>In the phone web interface, enter the delay in seconds.</li> </ul> <p>Valid values: An integer ranging from 1 through 300<br/>Default: 3</p> |
| DHCP VLAN Option      | <p>A predefined DHCP VLAN option to learn the voice VLAN ID. You can use the feature only when no voice VLAN information is available by CDP/LLDP and manual VLAN methods. CDP/LLDP and manual VLAN are all disabled.</p> <p>Set the value to Null to disable DHCP VLAN option. Cisco recommends that you use DHCP Option 132.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="1015 1266 1396 1323">&lt;DHCP_VLAN_Option ua="na"&gt;132&lt;/DHCP_VLAN_Option&gt;</pre> </li> <li>In the phone web page: specify the DHCP VLAN option.</li> </ul>   |

## SIP Configuration

SIP settings for the Cisco IP Phone are configured for the phone in general and for the extensions.

### Configure the Basic SIP Parameters

#### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

## Procedure

- 
- Step 1** Select **Voice > SIP**.
- Step 2** In the **SIP Parameters** section, set the parameters as described in the [SIP Parameters, on page 342](#) table.
- Step 3** Click **Submit All Changes**.
- 

## SIP Parameters

| Parameter       | Description  |
|-----------------|--|
| Max Forward     | <p>Specifies SIP Max Forward value.</p> <p>Perform one of the following.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:<br/> <pre>&lt;Max_Forward ua="na"&gt;70&lt;/Max_Forward&gt;</pre> </li> <li>In the phone web page, enter an appropriate value.</li> </ul> <p>Value range: 1 to 255<br/>Default: 70</p>   |
| Max Redirection | <p>Specifies number of times an invite can be redirected to avoid an infinite loop.</p> <p>Perform one of the following.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:<br/> <pre>&lt;Max_Redirection ua="na"&gt;5&lt;/Max_Redirection&gt;</pre> </li> <li>In the phone web page, enter an appropriate value.</li> </ul> <p>Default: 5</p>                 |
| Max Auth        | <p>Specifies the maximum number of times (from 0 to 255) a request can be challenged.</p> <p>Perform one of the following.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:<br/> <pre>&lt;Max_Auth ua="na"&gt;2&lt;/Max_Auth&gt;</pre> </li> <li>In the phone web page, enter an appropriate value.</li> </ul> <p>Allowed value: 0 to 255<br/>Default: 2</p> |



| Parameter               | Description   |
|-------------------------|---|
| SIP User Agent Name     | <p>Used in outbound requests.</p> <p>Perform one of the following.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;SIP_User_Agent_Name ua="na"&gt;\$VERSION&lt;/SIP_User_Agent_Name&gt;</pre> </li> <li>In the phone web page, enter an appropriate name.</li> </ul> <p>Default: \$VERSION</p> <p>If empty, the header is not included. Macro expansion of \$A to \$D corresponding to GPP_A to GPP_D allowed</p>   |
| SIP Server Name         | <p>Server header used in responses to inbound responses.</p> <p>Perform one of the following.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;SIP_Server_Name ua="na"&gt;\$VERSION&lt;/SIP_Server_Name&gt;</pre> </li> <li>In the phone web page, enter an appropriate name.</li> </ul> <p>Default: \$VERSION</p>   |
| SIP Reg User Agent Name | <p>User-Agent name to be used in a REGISTER request. If this is not specified, the SIP User Agent Name is also used for the REGISTER request.</p> <p>Perform one of the following.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;SIP_Reg_User_Agent_Name ua="na"&gt;agent name&lt;/SIP_Reg_User_Agent_Name&gt;</pre> </li> <li>In the phone web page, enter an appropriate name.</li> </ul> <p>Default: Blank</p> |
| SIP Accept Language     | <p>Accept-Language header used.</p> <p>Perform one of the following.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;SIP_Accept_Language ua="na"&gt;en&lt;/SIP_Accept_Language&gt;</pre> </li> <li>In the phone web page, enter an appropriate language.</li> </ul> <p>There is no default. If empty, the header is not included.</p>   |

| Parameter            | Description  |
|----------------------|--|
| DTMF Relay MIME Type | <p>MIME Type used in a SIP INFO message to signal a DTMF event. This field must match that of the Service Provider.</p> <p>Perform one of the following.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;DTMF_Relay_MIME_Type ua="na"&gt;application/dtmf-relay&lt;/DTMF_Relay_MIME_Type&gt;</pre> </li> <li>In the phone web page, enter an appropriate MIME type.</li> </ul> <p>Default: application/dtmf-relay</p>        |
| Hook Flash MIME Type | <p>MIME Type used in a SIPINFO message to signal a hook flash event.</p> <p>Perform one of the following.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;Hook_Flash_MIME_Type ua="na"&gt;application/hook-flash&lt;/Hook_Flash_MIME_Type&gt;</pre> </li> <li>In the phone web page, enter an appropriate MIME type for a SIPINFO message.</li> </ul> <p>Default:</p>  |
| Remove Last Reg      | <p>Enables you to remove the last registration before registering a new one if the value is different.</p> <p>Set to Yes to remove the last registration.</p> <p>Perform one of the following.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;Remove_Last_Reg ua="na"&gt;No&lt;/Remove_Last_Reg&gt;</pre> </li> <li>In the phone web page, Select Yes or No.</li> </ul> <p>Allowed values: Yes or No</p> <p>Default: No</p> |

| Parameter           | Description  |
|---------------------|--|
| Use Compact Header  | <p>If set to yes, the phone uses compact SIP headers in outbound SIP messages. If inbound SIP requests contain normal headers, the phone substitutes incoming headers with compact headers. If set to no, the phones use normal SIP headers. If inbound SIP requests contain compact headers, the phones reuse the same compact headers when generating the response, regardless of this setting.</p> <p>Perform one of the following.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="824 632 1474 653">&lt;Use_Compact_Header ua="na"&gt;No&lt;/Use_Compact_Header&gt;</pre> </li> <li>In the phone web page, select Yes or No.</li> </ul> <p>Allowed values: Yes or No<br/>Default: No</p> |
| Escape Display Name | <p>Enables you to keep the Display Name private.</p> <p>Set to Yes if you want the IP phone to enclose the string (configured in the Display Name) in a pair of double quotes for outbound SIP messages.</p> <p>Perform one of the following.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="824 1094 1498 1115">&lt;Escape_Display_Name ua="na"&gt;No&lt;/Escape_Display_Name&gt;</pre> </li> <li>In the phone web page, select Yes or No.</li> </ul> <p>Allowed values: Yes or No<br/>Default: Yes.</p>  |
| Talk Package        | <p>Enables support for the BroadSoft Talk Package that lets users answer or resume a call by clicking a button in an external application.</p> <p>Perform one of the following.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="824 1503 1320 1524">&lt;Talk_Package ua="na"&gt;No&lt;/Talk_Package&gt;</pre> </li> <li>In the phone web page, select Yes to enable the Talk Package.</li> </ul> <p>Allowed values: Yes or No<br/>Default: No</p>   |

| Parameter          | Description   |
|--------------------|---|
| Hold Package       | <p>Enables support for the BroadSoft Hold Package, which lets users place a call on hold by clicking a button in an external application.</p> <p>Perform one of the following.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:<br/> <pre>&lt;Hold_Package ua="na"&gt;No&lt;/Hold_Package&gt;</pre> </li> <li>In the phone web page, select Yes to enable support for the Hold Package.</li> </ul> <p>Allowed values: Yes or No<br/>Default: No</p>   |
| Conference Package | <p>Enables support for the BroadSoft Conference Package that enables users to start a conference call by clicking a button in an external application.</p> <p>Perform one of the following.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:<br/> <pre>&lt;Conference_Package ua="na"&gt;No&lt;/Conference_Package&gt;</pre> </li> <li>In the phone web page, select Yes or No.</li> </ul> <p>Allowed values: Yes or No<br/>Default: No</p>   |
| RFC 2543 Call Hold | <p>If set to yes, unit includes c=0.0.0.0 syntax in SDP when sending a SIP re-INVITE to the peer to hold the call. If set to no, unit will not include the c=0.0.0.0 syntax in the SDP. The unit will always include a=sendonly syntax in the SDP in either case.</p> <p>Perform one of the following.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:<br/> <pre>&lt;RFC_2543_Call_Hold ua="na"&gt;Yes&lt;/RFC_2543_Call_Hold&gt;</pre> </li> <li>In the phone web page, Yes or No.</li> </ul> <p>Allowed values: Yes or No<br/>Default: Yes</p> |

| Parameter                | Description  |
|--------------------------|--|
| Random REG CID on Reboot | <p>If set to yes, the phone uses a different random call-ID for registration after the next software reboot. If set to no, the Cisco IP phone tries to use the same call-ID for registration after the next software reboot. The Cisco IP phone always uses a new random Call-ID for registration after a power-cycle, regardless of this setting.</p> <p>Perform one of the following.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="824 604 1295 657">&lt;Random_REG_CID_on_Reboot ua="na"&gt;No&lt;/Random_REG_CID_on_Reboot&gt;</pre> </li> <li>In the phone web page, select Yes or No.</li> </ul> <p>Default: No.</p> |
| SIP TCP Port Min         | <p>Specifies the lowest TCP port number that can be used for SIP sessions.</p> <p>Perform one of the following.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="824 961 1450 993">&lt;SIP_TCP_Port_Min ua="na"&gt;5060&lt;/SIP_TCP_Port_Min&gt;</pre> </li> <li>In the phone web page, enter an appropriate value.</li> </ul> <p>Default: 5060</p>  |
| SIP TCP Port Max         | <p>Specifies the highest TCP port number that can be used for SIP sessions.</p> <p>Perform one of the following.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="824 1297 1450 1329">&lt;SIP_TCP_Port_Max ua="na"&gt;5080&lt;/SIP_TCP_Port_Max&gt;</pre> </li> <li>In the phone web page, enter an appropriate value.</li> </ul> <p>Default: 5080</p>   |

| Parameter                | Description  |
|--------------------------|--|
| Caller ID Header         | <p>Provides the option to take the caller ID from PAID-RPID-FROM, PAID-FROM, RPID-PAID-FROM, RPID-FROM, or FROM header.</p> <p>Perform one of the following.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="784 506 1308 562">&lt;Caller_ID_Header ua="na"&gt;PAID-RPID-FROM&lt;/Caller_ID_Header&gt;</pre> </li> <li>In the phone web page, select an option.</li> </ul> <p>Allowed values: PAID-RPID-FROM, AID-FROM, RPID-PAID-FROM, RPID-FROM, and FROM</p> <p>Default: PAID-RPID-FROM</p>                        |
| Hold Target Before Refer | <p>Controls whether to hold call leg with transfer target before sending REFER to the transferee when initiating a fully-attended call transfer (where the transfer target has answered).</p> <p>Perform one of the following.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="784 1010 1256 1066">&lt;Hold_Target_Before_Refer ua="na"&gt;No&lt;/Hold_Target_Before_Refer&gt;</pre> </li> <li>In the phone web page, select Yes or No.</li> </ul> <p>Default: No</p>   |
| Dialog SDP Enable        | <p>When enabled and the Notify message body is too big causing fragmentation, the Notify message xml dialog is simplified; Session Description Protocol (SDP) is not included in the dialog xml content.</p> <p>Perform one of the following.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="784 1436 1411 1463">&lt;Dialog_SDP_Enable ua="na"&gt;No&lt;/Dialog_SDP_Enable&gt;</pre> </li> <li>In the phone web page, select <b>Yes</b> or <b>No</b>.</li> </ul> <p>Allowed values: Yes or No</p> <p>Default: No</p> |

| Parameter                      | Description   |
|--------------------------------|---|
| Keep Referee When Refer Failed | <p>If set to yes, it configures the phone to immediately handle NOTIFY sipfrag messages.</p> <p>Perform one of the following.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="824 506 1373 558">&lt;Keep_Referee_When_Refer_Failed ua="na"&gt;No&lt;/Keep_Referee_When_Refer_Failed&gt;</pre> </li> <li>In the phone web page, select <b>Yes</b> or <b>No</b>.</li> </ul> <p>Allowed values: Yes or No<br/>Default: No</p>   |
| Display Diversion Info         | <p>Display the Diversion info included in SIP message on LCD or not.</p> <p>Perform one of the following.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="824 915 1271 968">&lt;Display_Diversion_Info ua="na"&gt;No&lt;/Display_Diversion_Info&gt;</pre> </li> <li>In the phone web page, select <b>Yes</b> or <b>No</b>.</li> </ul> <p>Allowed values: Yes or No</p>   |
| Display Anonymous From Header  | <p>Show the caller ID from the SIP INVITE message "From" header when set to Yes, even if the call is an anonymous call. When the parameter is set to no, the phone displays "Anonymous Caller" as the caller ID.</p> <p>Perform one of the following.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="824 1346 1360 1398">&lt;Display_Anonymous_From_Header ua="na"&gt;No&lt;/Display_Anonymous_From_Header&gt;</pre> </li> <li>In the phone web page, select <b>Yes</b> or <b>No</b>.</li> </ul> <p>Allowed values: Yes or No<br/>Default: No</p> |

| Parameter                    | Description   |
|------------------------------|---|
| Sip Accept Encoding          | <p>Supports the content-encoding gzip feature.</p> <p>If gzip is selected, the SIP message header contains the string “Accept-Encoding: gzip”, and the phone is able to process the SIP message body, which is encoded with the gzip format.</p> <p>Perform one of the following.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;Sip_Accept_Encoding ua="na"&gt;none&lt;/Sip_Accept_Encoding&gt;</pre> </li> <li>In the phone web page, enter an appropriate MIME type for a SIPINFO message.</li> </ul> <p>Allowed values: none and gzip</p> <p>Default: none</p> |
| SIP IP Preference            | <p>Sets if the phone uses IPv4 or IPv6.</p> <p>Perform one of the following.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;SIP_IP_Preference ua="na"&gt;IPv4&lt;/SIP_IP_Preference&gt;</pre> </li> <li>In the phone web page, select IPv4 or IPv6.</li> </ul> <p>Allowed values: IPv4/IPv6</p> <p>Default: IPv4.</p>  |
| Disable Local Name To Header | <p>Controls the display name in “Directory”, “Call History”, and in the “To” header during an outgoing call.</p> <p>Perform one of the following.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;Disable_Local_Name_To_Header ua="na"&gt;No&lt;/Disable_Local_Name_To_Header&gt;</pre> </li> <li>In the phone web page, select <b>Yes</b> to disable the display name.</li> </ul> <p>Allowed values: Yes/No</p> <p>Default: No</p>   |

## Configure the SIP Timer Values

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).



## Procedure

- 
- Step 1** Select **Voice > SIP**.
- Step 2** In the **SIP Timer Values** section, set the SIP timer values in seconds as described in [SIP Timer Values \(sec\)](#), on page 351.
- Step 3** Click **Submit All Changes**.
- 

## SIP Timer Values (sec)

| Parameter   | Description   |
|-------------|---|
| SIP T1      | RFC 3261 T1 value (RTT estimate) that can range from 0 to 64 seconds.<br>Default: 0.5 seconds   |
| SIP T2      | RFC 3261 T2 value (maximum retransmit interval for non-INVITE requests and INVITE responses) that can range from 0 to 64 seconds.<br>Default: 4 seconds |
| SIP T4      | RFC 3261 T4 value (maximum duration a message remains in the network), which can range from 0 to 64 seconds.<br>Default: 5 seconds.                     |
| SIP Timer B | INVITE time-out value, which can range from 0 to 64 seconds.<br>Default: 16 seconds.  |
| SIP Timer F | Non-INVITE time-out value, which can range from 0 to 64 seconds.<br>Default: 16 seconds.  |
| SIP Timer H | INVITE final response, time-out value, which can range from 0 to 64 seconds.<br>Default: 16 seconds.  |
| SIP Timer D | ACK hang-around time, which can range from 0 to 64 seconds.<br>Default: 16 seconds.   |
| SIP Timer J | Non-INVITE response hang-around time, which can range from 0 to 64 seconds.<br>Default: 16 seconds.   |

| Parameter                   | Description  |
|-----------------------------|--|
| INVITE Expires              | INVITE request Expires header value. If you enter 0, the Expires header is not included in the request. Ranges from 0 to 2000000.<br>Default: 240 seconds  |
| ReINVITE Expires            | ReINVITE request Expires header value. If you enter 0, the Expires header is not included in the request. Ranges from 0 to 2000000.<br>Default: 30   |
| Reg Min Expires             | Minimum registration expiration time allowed from the proxy in the Expires header or as a Contact header parameter. If the proxy returns a value less than this setting, the minimum value is used.  |
| Reg Max Expires             | Maximum registration expiration time allowed from the proxy in the Min-Expires header. If the value is larger than this setting, the maximum value is used.  |
| Reg Retry Intv              | Interval to wait before the Cisco IP Phone retries registration after failing during the last registration. The range is from 1 to 2147483647<br>Default: 30<br>See the note below for additional details.   |
| Reg Retry Long Intvl        | When registration fails with a SIP response code that does not match <Retry Reg RSC>, the Cisco IP Phone waits for the specified length of time before retrying. If this interval is 0, the phone stops trying. This value should be much larger than the Reg Retry Intvl value, which should not be 0.<br>Default: 1200<br>See the note below for additional details. |
| Reg Retry Random Delay      | Random delay range (in seconds) to add to <Register Retry Intvl> when retrying REGISTER after a failure. Minimum and maximum random delay to be added to the short timer. The range is from 0 to 2147483647.<br>Default: 0   |
| Reg Retry Long Random Delay | Random delay range (in seconds) to add to <Register Retry Long Intvl> when retrying REGISTER after a failure.<br>Default: 0  |

| Parameter           | Description  |
|---------------------|--|
| Reg Retry Intvl Cap | Maximum value of the exponential delay. The maximum value to cap the exponential backoff retry delay (which starts at the Register Retry Intvl and doubles every retry). Defaults to 0, which disables the exponential backoff (that is, the error retry interval is always at the Register Retry Intvl). When this feature is enabled, the Reg Retry Random Delay is added to the exponential backoff delay value. The range is from 0 to 2147483647.<br><br>Default: 0 |
| Sub Min Expires     | Sets the lower limit of the REGISTER expires value returned from the Proxy server.   |
| Sub Max Expires     | Sets the upper limit of the REGISTER minexpires value returned from the Proxy server in the Min-Expires header.<br><br>Default: 7200.  |
| Sub Retry Intvl     | This value (in seconds) determines the retry interval when the last Subscribe request fails.<br><br>Default: 10.   |



**Note** The phone can use a RETRY-AFTER value when it is received from a SIP proxy server that is too busy to process a request (503 Service Unavailable message). If the response message includes a RETRY-AFTER header, the phone waits for the specified length of time before to REGISTER again. If a RETRY-AFTER header is not present, the phone waits for the value specified in the Reg Retry Interval or the Reg Retry Long Interval.

## Configure the Response Status Code Handling

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

- 
- Step 1** Select **Voice > SIP**.
- Step 2** In the **Response Status Code Handling** section, set the values as specified in the [Response Status Code Handling Parameters, on page 354](#) table.
- Step 3** Click **Submit All Changes**.
-

## Response Status Code Handling Paramters

The following table defines the function and usage of the parameters in the Response Status Code Handling section under the SIP tab in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file with XML(cfg.xml) code to configure a parameter.

**Table 55: Response Status Code Handling Paramters**

| Parameter      | Description  |
|----------------|--|
| Try Backup RSC | <p>This parameter may be set to invoke failover upon receiving specified response codes.</p> <p>For example, you can enter numeric values 500 or a combination of numeric values plus wild cards if multiple values are possible. For the later, you can use 5?? to represent all SIP Response messages within the 500 range. If you want to use multiple ranges, you can add a comma "," to delimit values of 5?? and 6??</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:<br/> <pre>&lt;Try_Backup_RSC ua="na"/&gt;</pre> </li> <li>In the phone web page, enter an appropriate value.</li> </ul> <p>Default: Blank</p>             |
| Retry Reg RSC  | <p>Interval to wait before the phone retries registration after failing during the last registration.</p> <p>For example, you can enter numeric values 500 or a combination of numeric values plus wild cards if multiple values are possible. For the later, you can use 5?? to represent all SIP Response messages within the 500 range. If you want to use multiple ranges, you can add a comma "," to delimit values of 5?? and 6??</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:<br/> <pre>&lt;Retry_Reg_RSC ua="na"/&gt;</pre> </li> <li>In the phone web page, enter an appropriate value.</li> </ul> <p>Default: Blank</p> |

## Configure NTP Server

You can configure NTP servers with IPv4 and IPv6. You can also configure NTP server with DHCPv4 option 42 or DHCPv6 option 56. Configuring NTP with Primary NTP Server and Secondary NTP server parameters has higher priority over configuring NTP with DHCPv4 option 42 or DHCPv6 option 56.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

- 
- Step 1** Select **Voice > Systems**.
- Step 2** In the **Optional Network Configuration** section, set the IPv4 or IPv6 address as described in the [NTP Server Parameters, on page 355](#) table.
- Step 3** Click **Submit All Changes**.
- 

## NTP Server Parameters

The following table defines the function and usage of NTP server parameters in the Optional Network Configuration section under the System tab in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file with XML(cfg.xml) code to configure a parameter.

**Table 56: NTP Server Parameters**

| Parameter          | Description  |
|--------------------|--|
| Primary NTP Server | <p>IP address or name of the primary NTP server used to synchronize its time.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:           <pre>&lt;Primary_NTP_Server ua="rw"/&gt;</pre> </li> <li>In the phone web page, enter the IP address of the primary NTP server.</li> </ul> <p>Default: Blank</p> |

| Parameter            | Description   |
|----------------------|---|
| Secondary NTP Server | <p>IP address or name of the secondary NTP server used to synchronize its time.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:<br/> <pre>&lt;Secondary_NTP_Server ua="rw"/&gt;</pre> </li> <li>In the phone web page, enter the IP address of the secondary NTP server.</li> </ul> <p>Default: Blank</p> |

## Configure the RTP Parameters

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

- 
- Step 1** Select **Voice > SIP**.
- Step 2** In the **RTP Parameters** section, set the Real-Time Transport Protocol (RTP) parameter values as described in [RTP Parameters, on page 357](#).
- Step 3** Click **Submit All Changes**.
-

## RTP Parameters

The following table defines the function and usage of the parameters in the RTP Parameters section under the SIP tab in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file with XML(cfg.xml) code to configure a parameter.

**Table 57: RTP Parameters**

| Parameter    | Description   |
|--------------|---|
| RTP Port Min | <p>Minimum port number for RTP transmission and reception.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:           <pre>&lt;RTP_Port_Min ua="na"&gt;16384&lt;/RTP_Port_Min&gt;</pre> </li> <li>In the phone web page, enter an appropriate port number.</li> </ul> <p>Allowed values: 2048 to 49151</p> <p>If the value range (<b>RTP Port Max - RTP Port Min</b>) is less than 16 or you configure the parameter incorrectly, the RTP port range (16382 to 32766) is used instead.</p> <p>Default: 16384</p> |
| RTP Port Max | <p>Maximum port number for RTP transmission and reception.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:           <pre>&lt;RTP_Port_Max ua="na"&gt;16482&lt;/RTP_Port_Max&gt;</pre> </li> <li>In the phone web page, enter an appropriate port number.</li> </ul> <p>Allowed values: 2048 to 49151</p> <p>If the value range (<b>RTP Port Max - RTP Port Min</b>) is less than 16 or you configure the parameter incorrectly, the RTP port range (16382 to 32766) is used instead.</p> <p>Default: 16482</p> |

| Parameter        | Description  |
|------------------|--|
| RTP Packet Size  | <p>Specifies packet size in seconds.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="974 472 1356 525">&lt;RTP_Packet_Size ua="na"&gt;0.02&lt;/RTP_Packet_Size&gt;</pre> </li> <li>In the phone web page, enter an appropriate value to specify the packet size.</li> </ul> <p>Allowed values: Ranges from 0.01 to 0.13. Valid values must be a multiple of 0.01 seconds.</p> <p>Default: 0.02</p>                           |
| Max RTP ICMP Err | <p>Number of successive ICMP errors allowed when transmitting RTP packets to the peer before the phone terminates the call. If value is set to 0, the phone ignores the limit on ICMP errors.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="974 1039 1331 1092">&lt;Max_RTP_ICMP_Err ua="na"&gt;0&lt;/Max_RTP_ICMP_Err&gt;</pre> </li> <li>In the phone web page, enter an appropriate value.</li> </ul> <p>Default: 0</p> |
| RTCP Tx Interval | <p>Interval for sending out RTCP sender reports on an active connection.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="974 1459 1331 1512">&lt;RTCP_Tx_Interval ua="na"&gt;5&lt;/RTCP_Tx_Interval&gt;</pre> </li> <li>In the phone web page, enter an appropriate value.</li> </ul> <p>Allowed values: 0 to 255 seconds</p> <p>Default: 0</p>  |



| Parameter          | Description   |
|--------------------|---|
| Call Statistics    | <p>Specifies whether the phone sends end-of-call statistics within SIP messages when a call terminates or is put on hold.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="1015 535 1372 598">&lt;Call_Statistics ua="na"&gt;No&lt;/Call_Statistics&gt;</pre> </li> <li>In the phone web page, select <b>Yes</b> to enable this feature.</li> </ul> <p>Allowed values: Yes and No<br/>Default: No</p>  |
| SDP IP Preferences | <p>Select the preferred IP that the phone uses as RTP address.</p> <p>If the phone is in dual-mode and has both ipv4 and ipv6 addresses, it will always include both addresses in SDP by attributes "a=altc ...</p> <p>If IPv4 address is selected, then ipv4 address has higher priority than ipv6 address in SDP and indicates that phone prefers using ipv4 RTP address.</p> <p>If the phone has only ipv4 address or ipv6 address, SDP does not have ALTC attributes and RTP address is specified in "c=" line.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="1015 1344 1421 1396">&lt;SDP_IP_Preference ua="na"&gt;IPv4&lt;/SDP_IP_Preference&gt;</pre> </li> <li>In the phone web page, select the preferred IP .</li> </ul> <p>Allowed values: IPv4 and IPv6<br/>Default: IPv4</p> |

| Parameter               | Description   |
|-------------------------|---|
| RTP Before ACK          | <p>Allows you to specify whether an RTP session starts before or after an ACK is received from the calling party.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="976 537 1321 590">&lt;RTP_Before_ACK ua="na"&gt;No&lt;/RTP_Before_ACK&gt;</pre> </li> <li>In the phone web page select: <ul style="list-style-type: none"> <li><b>Yes:</b> An RTP session doesn't await an ACK, but starts after a 200 OK message is sent.</li> <li><b>No:</b> An RTP session doesn't start until an ACK is received from the calling party.</li> </ul> </li> </ul> <p>Allowed values: Yes and No</p> <p>Default: No</p>  |
| SSRC Reset on RE-INVITE | <p>Controls whether to reset the Synchronization Source (SSRC) for the new RTP and SRTP sessions.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="976 1161 1446 1213">&lt;SSRC_Reset_on_RE-INVITE ua="na"&gt;Yes&lt;/SSRC_Reset_on_RE-INVITE&gt;</pre> </li> <li>In the phone web page select: <ul style="list-style-type: none"> <li><b>Yes:</b> the phone can avoid the call transfer error, where only one person on the call hears the audio. This occurs on calls of 30 minutes or longer, and often on three-way calls.</li> <li><b>No:</b> the SSRC still remains during a long duration call. In this case, this error might occur.</li> </ul> </li> </ul> <p>Allowed values: Yes and No</p> <p>Default: No</p> |

## Enable SSRC Reset for the New RTP and SRTP Sessions

You can enable the **SSRC Reset on RE-INVITE** to avoid a call transfer error, where only one person on the call hears the audio. This error occurs on calls of 30 minutes or longer, and often on three-way calls.

**Before you begin**

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

**Procedure**

- 
- Step 1** Select **Voice > SIP**.
- Step 2** In the **RTP Parameters** section, set the parameter **SSRC Reset on RE-INVITE** to **Yes**.
- You can also configure this parameter in the configuration file:
- ```
<SSRC_Reset_on_RE-INVITE ua="na">Yes</SSRC_Reset_on_RE-INVITE>
```
- Allowed values: Yes and No.
- Default: No
- Note** If you set the parameter to **No**, the SSRC remains for the new RTP and SRTP sessions (SIP re-INVITES). The call transfer error might occur during a long duration call.
- Step 3** Click **Submit All Changes**.
- 

## Control SIP and RTP Behaviour in Dual Mode

You can control SIP and RTP parameters with SIP IP Preference and SDP IP Preference fields when phone is in dual mode.

SIP IP Preference parameter defines which IP address phone tries first when it is in dual mode.

*Table 58: SIP IP Preference and IP Mode*

IP Mode	SIP IP Preference	Address List from DNS, Priority, Result P1 - First Priority Address P2 - Second Priority Address	Failover Sequence
Dual Mode	IPv4	P1- 1.1.1.1, 2009:1:1:1::1 P2 - 2.2.2.2, 2009:2:2:2::2 <b>Result:</b> Phone will send the SIP messages to 1.1.1.1 first.	1.1.1.1 ->2009:1:1:1 -> 2.2.2.2 -> 2009:2:2:2
Dual Mode	IPv6	P1- 1.1.1.1, 2009:1:1:1::1 P2 - 2.2.2.2, 2009:2:2:2::2 <b>Result:</b> Phone will send the SIP messages to 2009:1:1:1::1 first.	2009:1:1:1:1 -> 1.1.1.1 -> 2009:2:2:2:2 -> 2.2.2.2

IP Mode	SIP IP Preference	Address List from DNS, Priority, Result P1 - First Priority Address P2 - Second Priority Address	Failover Sequence
Dual Mode	IPv4	P1- 2009:1:1:1::1 P2 - 2.2.2.2, 2009:2:2:2::2 <b>Result:</b> Phone will send the SIP messages to 2009:1:1:1::1 first.	2009:1:1:1:1 -> 2.2.2.2 -> 2009:2:2:2:2
Dual Mode	IPv6	P1- 2009:1:1:1::1 P2 - 2.2.2.2, 2009:2:2:2::2 <b>Result:</b> Phone will send the SIP messages to 1.1.1.1 first.	2009:1:1:1:1 -> 2009:2:2:2:2 -> 2.2.2.2
IPv4 Only	IPv4 or IPv6	P1 - 1.1.1.1, 2009:1:1:1::1 P2 - 2.2.2.2, 2009:2:2:2::2 <b>Result:</b> Phone will send the SIP messages to 1.1.1.1 first.	1.1.1.1 -> 2.2.2.2
IPv6 Only	IPv4 or IPv6	P1 - 1.1.1.1, 2009:1:1:1::1 P2 - 2.2.2.2, 2009:2:2:2::2 <b>Result:</b> Phone will send the SIP messages to 2009:1:1:1::1 first.	2009:1:1:1:1 -> 2009:2:2:2:2

SDP IP Preference - ALTC helps peers in dual-mode negotiate RTP address family.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

- 
- Step 1** Select **Voice > SIP**.
- Step 2** In the **SIP Parameters** section, select **IPv4** or **IPv6** in the **SIP IP Preference** field.  
For details, see **SDP IP Preference** field in the [SIP Parameters, on page 342](#) table.
- Step 3** In the **RTP Parameters** section, select **IPv4** or **IPv6** in the **SDP IP Preference** field.  
For details, see **SDP IP Preference** in the [RTP Parameters, on page 357](#) table.
-

## Configure the SDP Payload Types

Your Cisco IP Phone supports RFC4733. You can choose from three audio-video transport (AVT) options to send DTMF pulses to the server.

Configured dynamic payloads are used for outbound calls only when the Cisco IP Phone presents a Session Description Protocol (SDP) offer. For inbound calls with an SDP offer, the phone follows the caller's assigned dynamic payload type.

The Cisco IP Phone uses the configured codec names in outbound SDP. For incoming SDP with standard payload types of 0-95, the phone ignores the codec names. For dynamic payload types, the phone identifies the codec by the configured codec names. The comparison is case-sensitive, so you need to set the name correctly.

You can also configure the parameters in the phone configuration file (cfg.xml). To configure each of the parameters, see the syntax of the string in [SDP Payload Types, on page 364](#).

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

- 
- Step 1** Select **Voice > SIP**.
- Step 2** In the **SDP Payload Types** section, set the value as specified in [SDP Payload Types, on page 364](#).
- **AVT Dynamic Payload**—is any nonstandard data. Both sender and receiver must agree on a number. The range is from 96 to 127. The default is 101.
  - **AVT 16kHz Dynamic Payload** —is any nonstandard data. Both sender and receiver must agree on a number. The range is from 96 to 127. The default is 107.
  - **AVT 48kHz Dynamic Payload** —is any nonstandard data. Both sender and receiver must agree on a number. The range is from 96 to 127. The default is 108.
- Step 3** Click **Submit All Changes**.
-

## SDP Payload Types

Parameter	Description
G722.2 Dynamic Payload	<p>G722 Dynamic Payload type.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;Try_Backup_RSC ua="na"/&gt;</pre> </li> <li>In the phone web page, enter an appropriate value.</li> </ul> <p>Allowed values: Default: 96</p>
iLBC Dynamic Payload	<p>iLBC Dynamic Payload type.</p> <p>Default: 97</p>
OPUS Dynamic Payload	<p>OPUS Dynamic Payload type.</p> <p>Default: 99</p>
AVT Dynamic Payload	<p>AVT dynamic payload type. Ranges from 96-127.</p> <p>Default: 101</p>
INFOREQ Dynamic Payload	<p>INFOREQ Dynamic Payload type.</p>
H264 BP0 Dynamic Payload	<p>H264 BPO Dynamic Payload type.</p> <p>Default: 110</p>
H264 HP Dynamic Payload	<p>H264 HP Dynamic Payload type.</p> <p>Default: 110</p>
G711u Codec Name	<p>G711u codec name used in SDP.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;G711u_Codec_Name ua="na"&gt;PCMU&lt;/G711u_Codec_Name&gt;</pre> </li> <li>In the phone web page, enter an appropriate codec name.</li> </ul> <p>Allowed values: Default: PCMU</p>

Parameter	Description
G711a Codec Name	<p>G711a codec name used in SDP.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="1013 474 1409 527">&lt;G711a_Codec_Name ua="na"&gt;PCMU&lt;/G711a_Codec_Name&gt;</pre> </li> <li>In the phone web page, enter an appropriate codec name.</li> </ul> <p>Allowed values: Default: PCMA</p>
G729a Codec Name	<p>G729a codec name used in SDP.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="1013 915 1409 968">&lt;G729a_Codec_Name ua="na"&gt;PCMU&lt;/G729a_Codec_Name&gt;</pre> </li> <li>In the phone web page, enter an appropriate codec name.</li> </ul> <p>Allowed values: Default: G729a</p>
G729b Codec Name	<p>G729b codec name used in SDP.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="1013 1356 1409 1409">&lt;G729b_Codec_Name ua="na"&gt;PCMU&lt;/G729b_Codec_Name&gt;</pre> </li> <li>In the phone web page, enter an appropriate codec name.</li> </ul> <p>Allowed values: Default: G729b</p>

Parameter	Description
G722 Codec Name	<p>G722 codec name used in SDP.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="976 474 1360 527">&lt;G722_Codec_Name ua="na"&gt;PCMU&lt;/G722_Codec_Name&gt;</pre> </li> <li>In the phone web page, enter an appropriate codec name.</li> </ul> <p>Allowed values:</p> <p>Default: G722</p>
G722.2 Codec Name	<p>G722.2 codec name used in SDP.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="976 915 1386 968">&lt;G722.2_Codec_Name ua="na"&gt;PCMU&lt;/G722.2_Codec_Name&gt;</pre> </li> <li>In the phone web page, enter an appropriate codec name.</li> </ul> <p>Allowed values:</p> <p>Default: G722.2</p>
iLBC Codec Name	<p>iLBC codec name used in SDP.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="976 1356 1360 1409">&lt;iLBC_Codec_Name ua="na"&gt;iLBC&lt;/iLBC_Codec_Name&gt;</pre> </li> <li>In the phone web page, enter an appropriate codec name.</li> </ul> <p>Allowed values:</p> <p>Default: iLBC</p>



Parameter	Description
OPUS Codec Name	<p>OPUS codec name used in SDP.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="1015 472 1404 535">&lt;OPUS_Codec_Name ua="na"&gt;OPUS&lt;/OPUS_Codec_Name&gt;</pre> </li> <li>In the phone web page, enter an appropriate codec name.</li> </ul> <p>Allowed values:</p> <p>Default: OPUS</p>
AVT Codec Name	<p>AVT codec name used in SDP.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="1015 913 1518 976">&lt;AVT_Codec_Name ua="na"&gt;telephone-event&lt;/AVT_Codec_Name&gt;</pre> </li> <li>In the phone web page, enter an appropriate codec name.</li> </ul> <p>Allowed values:</p> <p>Default: telephone-event</p>
AVT 16 kHz Dynamic Payload	<p>AVT dynamic payload type for the 16 kHz clock rate.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="1015 1354 1518 1417">&lt;AVT_16kHz_Dynamic_Payload ua="na"&gt;107&lt;/AVT_16kHz_Dynamic_Payload&gt;</pre> </li> <li>In the phone web page, enter the payload.</li> </ul> <p>Range: 96-127</p> <p>Default: 107</p>

Parameter	Description
AVT 48 kHz Dynamic Payload	<p>AVT dynamic payload type for the 48 kHz clock rate.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;AVT_48kHz_Dynamic_Payload ua="na"&gt;108&lt;/AVT_48kHz_Dynamic_Payload&gt;</pre> </li> <li>In the phone web page, enter the payload.</li> </ul> <p>Range: 96-127</p> <p>Default: 108</p>

## Configure the SIP Settings for Extensions

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

- 
- Step 1** Select **Voice > Ext(n)**, where n is an extension number.
- Step 2** In the **SIP Settings** section, set the parameter values as described in the [Parameters for SIP Settings on Extensions, on page 369](#) table.
- Step 3** Click **Submit All Changes**.
-

## Parameters for SIP Settings on Extensions

The following table defines the function and usage of the parameters in the SIP Settings section under the Ext(n) tab in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file with XML(cfg.xml) code to configure a parameter.

**Table 59: SIP Settings in Extensions**

Parameter	Description
SIP Transport	<p>Specifies the transport protocol for SIP messages.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>• In the phone configuration file with XML(cfg.xml), enter a string in this format:           <pre data-bbox="1013 705 1398 762">&lt;SIP_Transport_1_ua="na"&gt;UDP&lt;/SIP_Transport_1_&gt;</pre> </li> <li>• In the phone web page, select the transport protocol type.           <ul style="list-style-type: none"> <li>• UDP</li> <li>• TCP</li> <li>• TLS</li> <li>• AUTO</li> </ul> </li> </ul> <p><b>AUTO</b> allows the phone to select the appropriate protocol automatically, based on the NAPTR records on the DNS server. See <a href="#">Configure the SIP Transport, on page 189</a> for more details.</p> <p>Default: UDP</p>

Parameter	Description
SIP Port	<p>The phone's port number for SIP message listening and transmission.</p> <p><b>Note</b> Specify the port number here only when you are using UDP as the SIP transport protocol.</p> <p>If you are using TCP, the system uses a random port within the range specified in <b>SIP TCP Port Min</b> and <b>SIP TCP Port Max</b> on the <b>Voice &gt; SIP</b> tab.</p> <p>If you need to specify a port of SIP proxy server, you can specify it using the <b>Proxy</b> field or the <b>XSI Host Server</b> field.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>• In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;SIP_Port_1_ ua="na"&gt;5060&lt;/SIP_Port_1_&gt;</pre> </li> <li>• In the phone web page, enter an appropriate port number.</li> </ul> <p>Default: 5060</p>
SIP 100REL Enable	<p>Individually enables the SIP 100REL feature.</p> <p>When enabled, the phone supports the 100REL SIP extension for reliable transmission of provisional responses (18x) and uses the PRACK requests.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>• In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;SIP_100REL_Enable_1_ ua="na"&gt;Yes&lt;/SIP_100REL_Enable_1_&gt;</pre> </li> <li>• In the phone web page, select Yes to enable the feature.</li> </ul> <p>Allowed values: Yes and No</p> <p>Default: No</p>

Parameter	Description
Precondition Support	<p>Determines whether the phone includes the precondition tag (defined in RFC 3312) in the Supported header field.</p> <ul style="list-style-type: none"> <li>• <b>Disabled:</b> The phone doesn't include the precondition tag in the Supported header field. And the phone doesn't return the 183 response when it receives the INVITE request that contains the QoS precondition in the SDP description.</li> <li>• <b>Enabled:</b> The phone includes the precondition tag in the Supported header field.</li> </ul> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>• In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="1015 842 1523 898">&lt;Precondition_Support_1_ua="na"&gt;Enabled&lt;/Precondition_Support_1_&gt;</pre> </li> <li>• In the phone web page, select <b>Enabled</b> to enable the feature.</li> </ul> <p>Allowed values: Disabled and Enabled Default: Disabled</p>
EXT SIP Port	<p>The external SIP port number.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>• In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="1015 1283 1398 1339">&lt;EXT_SIP_Port_1_ua="na"&gt;5060&lt;/EXT_SIP_Port_1_&gt;</pre> </li> <li>• In the phone web page, enter a port number.</li> </ul> <p>Allowed values: Default: 5060</p>

Parameter	Description
Auth Resync-Reboot	<p>The Cisco IP Phone authenticates the sender when it receives a NOTIFY message with the following requests:</p> <ul style="list-style-type: none"> <li>• resync</li> <li>• reboot</li> <li>• report</li> <li>• restart</li> <li>• XML-service</li> </ul> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>• In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="974 808 1412 861">&lt;Auth_Resync-Reboot_1_ ua="na"&gt;No&lt;/Auth_Resync-Reboot_1_&gt;</pre> </li> <li>• In the phone web page, select Yes to enable the feature.</li> </ul> <p>Allowed values: Yes and No Default: Yes</p>
SIP Proxy-Require	<p>The SIP proxy can support a specific extension or behavior when it receives the Proxy-Require header from the user agent. If this field is configured and the proxy does not support it, it responds with the message, unsupported.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>• In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="974 1375 1437 1428">&lt;SIP_Proxy-Require_1_ ua="na"&gt;header&lt;SIP_Proxy-Require_1_&gt;</pre> </li> <li>• In the phone web interface, enter the appropriate header in the field provided.</li> </ul> <p>Default: Blank</p>
SIP Remote-Party-ID	<p>The Remote-Party-ID header to use instead of the From header. Select <b>Yes</b> to enable.</p> <p>Default: Yes</p>

Parameter	Description
Referor Bye Delay	<p>Controls when the phone sends BYE to terminate stale call legs upon completion of call transfers. Multiple delay settings (Referor, Refer Target, Referee, and Refer-To Target) are configured on this screen.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="1013 569 1425 625">&lt;Referor_Bye_Delay_1_ua="na"&gt;4&lt;/Referor_Bye_Delay_1_&gt;</pre> </li> <li>In the phone web page, enter the appropriate period of time in seconds.</li> </ul> <p>Allowed values: An integer from 0 through 65535 Default: 4</p>
Refer-To Target Contact	<p>Indicates the refer-to target.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="1013 1010 1511 1066">&lt;Refer-To_Target_Contact_1_ua="na"&gt;No&lt;/Refer-To_Target_Contact_1_&gt;</pre> </li> <li>In the phone web page, select <b>Yes</b> to send the <b>SIP Refer</b> to the contact.</li> </ul> <p>Allowed values: Yes and No Default: No</p>
Referee Bye Delay	<p>Specifies the Referee Bye Delay time in seconds.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="1013 1451 1425 1507">&lt;Referee_Bye_Delay_1_ua="na"&gt;0&lt;/Referee_Bye_Delay_1_&gt;</pre> </li> <li>In the phone web page, enter the appropriate period of time in seconds.</li> </ul> <p>Allowed values: An integer from 0 through 65535 Default: 0</p>

Parameter	Description
Refer Target Bye Delay	<p>Specifies the Refer Target Bye Delay time in seconds.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="974 472 1453 535">&lt;Refer_Target_Bye_Delay_1_ua="na"&gt;0&lt;/Refer_Target_Bye_Delay_1_&gt;</pre> </li> <li>In the phone web page, enter the appropriate period of time in seconds.</li> </ul> <p>Allowed values: An integer from 0 through 65535 Default: 0</p>
Sticky 183	<p>Controls the first 183 SIP response for an outbound INVITE. To enable this feature,</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="974 945 1477 976">&lt;Sticky_183_1_ua="na"&gt;No&lt;/Sticky_183_1_&gt;</pre> </li> <li>In the phone web page, select <b>Yes</b> to enable this feature.</li> </ul> <p>When enabled, the IP telephony ignores further 180 SIP responses after receiving the first 183 SIP response for an outbound INVITE.</p> <p>Allowed values: Yes and No Default: No</p>



Parameter	Description
Auth INVITE	<p>Controls if authorization is required for initial incoming INVITE requests from the SIP proxy. To enable this feature.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="1015 535 1364 598">&lt;Auth_INVITE_1_ ua="na"&gt;No&lt;/Auth_INVITE_1_&gt;</pre> </li> <li>In the phone web page, select <b>Yes</b> to enable this feature.</li> </ul> <p>When enabled, authorization is required for initial incoming INVITE requests from the SIP proxy.</p> <p>Allowed values: Yes and No Default: No</p>
Ntfy Refer On 1xx-To-Inv	<p>If set to <b>Yes</b>, as a transferee, the phone will send a NOTIFY with Event:Refer to the transferor for any 1xx response returned by the transfer target, on the transfer call leg.</p> <p>If set to <b>No</b>, the phone will only send a NOTIFY for final responses (200 and higher).</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="1015 1270 1518 1333">&lt;Ntfy_Refer_On_1xx-To-Inv_1_ ua="na"&gt;Yes&lt;/Ntfy_Refer_On_1xx-To-Inv_1_&gt;</pre> </li> <li>In the phone web page, select <b>Yes</b> to enable this feature.</li> </ul> <p>Allowed values: Yes and No Default: Yes</p>

Parameter	Description
Set G729 annexb	<p>Configure G.729 Annex B settings.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="974 472 1388 535">&lt;Set_G729_annexb_1_ua="na"&gt;Yes&lt;/Set_G729_annexb_1_&gt;</pre> </li> <li>In the phone web page, select <b>Yes</b> to enable this feature.</li> </ul> <p>Allowed values:</p> <ul style="list-style-type: none"> <li>None</li> <li>No</li> <li>Yes</li> <li>Follow silence supp setting</li> </ul> <p>Default: Yes</p>
User Equal Phone	<p>When a tel URL is converted to a SIP URL and the phone number is represented by the user portion of the URL, the SIP URL includes the optional: user=phone parameter (RFC3261). For example: To: sip:+12325551234@example.com; user=phone</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="974 1270 1404 1333">&lt;User_Equal_Phone_1_ua="na"&gt;Yes&lt;/User_Equal_Phone_1_&gt;</pre> </li> <li>In the phone web page, select <b>Yes</b> to enable this feature.</li> </ul> <p>Allowed values: Yes and No</p> <p>Default: No</p>

Parameter	Description
Call Recording Protocol	<p>Determines the type of recording protocol that the phone uses. Options are:</p> <ul style="list-style-type: none"><li>• SIPINFO</li><li>• SIPREC</li></ul> <p>Perform one of the following:</p> <ul style="list-style-type: none"><li>• In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;Call_Recording_Protocol_1_ua="na"&gt;SIPREC&lt;/Call_Recording_Protocol_1_&gt;</pre></li><li>• In the phone web page, select a protocol from the list.</li></ul> <p>Allowed values: SIPREC SIPINFO Default: SIPREC</p>

Parameter	Description
Privacy Header	<p>Sets user privacy in the SIP message in the trusted network.</p> <p>The privacy header options are:</p> <ul style="list-style-type: none"> <li>• Disabled (default)</li> <li>• none—The user requests that a privacy service applies no privacy functions to this SIP message.</li> <li>• header—The user needs a privacy service to obscure headers which cannot be purged of identifying information.</li> <li>• session—The user requests that a privacy service provide anonymity for the sessions.</li> <li>• user—The user requests a privacy level only by intermediaries.</li> <li>• id—The user requests that the system substitute an id that doesn't reveal the IP address or host name.</li> </ul> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>• In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="974 1098 1437 1155">&lt;Privacy_Header_1_ua="na"&gt;Disabled&lt;/Privacy_Header_1_&gt;</pre> </li> <li>• In the phone web page, select an option from the list.</li> </ul> <p>Allowed values: Disabled none header session user id Default: Disabled</p>
P-Early-Media Support	<p>Controls whether the P-Early-Media header is included in the SIP message for an outgoing call.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>• In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="974 1570 1448 1627">&lt;P-Early-Media_Support_1_ua="na"&gt;No&lt;/P-Early-Media_Support_1_&gt;</pre> </li> <li>• In the phone web interface, to include the P-Early-Media header, select <b>Yes</b>.</li> </ul> <p>Allowed values: Yes and No Default: No</p>

## Configure the SIP Proxy Server

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

- 
- Step 1** Select **Voice > Ext(n)**, where n is an extension number.
- Step 2** In the **Proxy and Registration** section, set the parameter values as described in the [SIP Proxy and Registration for Extension Parameters, on page 379](#) table.
- Step 3** Click **Submit All Changes**.
- 

## SIP Proxy and Registration for Extension Parameters

The following table defines the function and usage of the parameters in the Proxy and Registration section under the Ext(n) tab in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file with XML(cfg.xml) code to configure a parameter.

*Table 60: SIP Proxy and Registration for Extension*

Parameter	Description
Proxy	<p>SIP proxy server and port number set by the service provider for all outbound requests. For example: 192.168.2.100:6060.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:           <pre>&lt;Proxy_1_ ua="na"&gt;64.101.154.134&lt;/Proxy_1_&gt; &lt;RTP_Port_Max ua="na"&gt;16482&lt;/RTP_Port_Max&gt;</pre> </li> <li>In the phone web page, enter SIP proxy server and port number.</li> </ul> <p>When you need to refer to this proxy in another setting, for example, the speed dial line key configuration, use the \$PROXY macro variable.</p> <p>Default: The port number is optional. If you don't specify a port, the default port 5060 is used for UDP, and the default port 5061 is used for TLS.</p>

Parameter	Description
Outbound Proxy	<p>Specifies an IP address or domain name. All outbound requests are sent as the first hop.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="781 457 1284 512">&lt;Outbound_Proxy_1_ ua="na"&gt;10.79.78.45&lt;/Outbound_Proxy_1_&gt;</pre> </li> <li>In the phone web page, enter an IP address and a domain name.</li> </ul> <p>Default: Empty</p>
Proxy Outbound Proxy <b>For Survivable Remote Site Telephony (SRST) support</b>	<p>These parameters can be configured with an extension that includes a statically-configured DNS SRV record or DNS A record. This allows for failover and fallback functionality with a secondary proxy server.</p> <p>The format for the parameter value is as follows:</p> <p>FQDN format: <code>hostname[:port][:SRV=host-list OR :A=ip-list]</code></p> <p>Where:</p> <ul style="list-style-type: none"> <li>host-list: <code>srv[ srv[ srv...]]</code></li> <li>srv: <code>hostname[:port][:p=priority][:weight][:A=ip-list]</code></li> <li>ip-list: <code>ip-addr[,ip-addr[,ip-addr...]]</code></li> </ul> <p>Default:</p> <ul style="list-style-type: none"> <li>Priority is 0.</li> <li>Weight is 1.</li> <li>Port is 5060 and 5061 for UDP and TLS respectively.</li> </ul>

Parameter	Description
Alternate Proxy Alternate Outbound Proxy	<p>This feature provides fast fall back when there is network partition at the Internet or when the primary proxy (or primary outbound proxy) is not responsive or available. The feature works well in a Verizon deployment environment as the alternate proxy is the Integrated Service Router (ISR) with analog outbound phone connection.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:               <pre data-bbox="824 554 1523 638">&lt;Alternate_Proxy_1_ua="na"&gt;10.74.23.43&lt;/Alternate_Proxy_1_&gt;&lt;Alternate_Outbound_Proxy_1_ua="na"&gt;10.74.23.44&lt;/Alternate_Outbound_Proxy_1_&gt;</pre> </li> <li>In the phone web page, enter the proxy server addresses and port numbers in these fields.</li> </ul> <p>After the phone is registered to the primary proxy and the alternate proxy (or primary outbound proxy and alternate outbound proxy), the phone always sends out INVITE and Non-INVITE SIP messages (except registration) via the primary proxy. The phone always registers to both the primary and alternate proxies. If there is no response from the primary proxy after timeout (per the SIP RFC spec) for a new INVITE, the phone attempts to connect with the alternate proxy. The phone always tries the primary proxy first, and immediately tries the alternate proxy if the primary is unreachable.</p> <p>Active transactions (calls) never fall back between the primary and alternate proxies. If there is fall back for a new INVITE, the subscribe/notify transaction will fall back accordingly so that the phone's state can be maintained properly. You must also set Dual Registration in the Proxy and Registration section to Yes.</p> <p>Default: Empty</p>
Use OB Proxy In Dialog	<p>Determines whether to force SIP requests to be sent to the outbound proxy within a dialog.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:               <pre data-bbox="824 1440 1321 1495">&lt;Use_OB_Proxy_In_Dialog_1_ua="na"&gt;Yes&lt;/Use_OB_Proxy_In_Dialog_1_&gt;</pre> </li> <li>In the phone web page, select <b>Yes</b> or <b>No</b>. The request is ignored if the <b>Use Outbound Proxy</b> field is set to <b>No</b> or if the <b>Outbound Proxy</b> field is empty.</li> </ul> <p>Valid values: Yes and No</p> <p>Default: Yes</p>

Parameter	Description
Register	<p>Enables periodic registration with the proxy. This parameter is ignored if a proxy is not specified.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;Register_1_ ua="na"&gt;Yes&lt;/Register_1_&gt;</pre> </li> <li>In the phone web page, To enable this feature, select <b>Yes</b>.</li> </ul> <p>Valid values: Yes and No  Default: Yes</p>
Make Call Without Reg	<p>Enables making outbound calls without successful (dynamic) registration by the phone.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;Make_Call_Without_Reg_1_ ua="na"&gt;No&lt;/Make_Call_Without_Reg_1_&gt;</pre> </li> <li>In the phone web page, To enable this feature, select <b>Yes</b>. If set to <b>No</b>, the dial tone plays only when registration is successful.</li> </ul> <p>Valid values: Yes and No  Default: No</p>
Register Expires	<p>Defines how often the phone renews registration with the proxy. If the proxy responds to a REGISTER with a lower expires value, the phone renews registration based on that lower value instead of the configured value.</p> <p>If registration fails with an “Expires too brief” error response, the phone retries with the value specified in the Min-Expires header of the error.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;Register_Expires_1_ ua="na"&gt;3600&lt;/Register_Expires_1_&gt;</pre> </li> <li>In the phone web page, enter a value in seconds to define how often the phone renews registration with the proxy.</li> </ul> <p>Valid values: Numeric. The range is from 32 seconds to 200000 seconds.  Default: 3600 seconds</p>



Parameter	Description
Ans Call Without Reg	<p>If enabled, the user does not have to be registered with the proxy to answer calls.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="824 457 1284 512">&lt;Ans_Call_Without_Reg_1_ ua="na"&gt;No&lt;/Ans_Call_Without_Reg_1_&gt;</pre> </li> <li>In the phone web page, To enable this feature, select <b>Yes</b>.</li> </ul> <p>Valid values: Yes and No Default: No</p>
Use DNS SRV	<p>Enables DNS SRV lookup for the proxy and outbound proxy.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="824 821 1386 842">&lt;Use_DNS_SRV_1_ ua="na"&gt;Yes&lt;/Use_DNS_SRV_1_&gt;</pre> </li> <li>In the phone web page, To enable this feature, select <b>Yes</b>.</li> </ul> <p>Valid values: Yes and No Default: No</p>
DNS SRV Auto Prefix	<p>Enables the phone to automatically append a prefix to the proxy or outbound proxy name when performing a DNS SRV lookup on that name. The prefix to be appended varies with SIP transport protocols.</p> <ul style="list-style-type: none"> <li>_sip._udp. for UDP protocol</li> <li>_sip._tcp. for TCP protocol</li> <li>_sips._tcp. for TLS protocol</li> </ul> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="824 1430 1284 1484">&lt;DNS_SRV_Auto_Prefix_1_ ua="na"&gt;Yes&lt;/DNS_SRV_Auto_Prefix_1_&gt;</pre> </li> <li>In the phone web page, to enable this feature, select <b>Yes</b>.</li> </ul> <p>Valid values: Yes and No Default: No</p>

Parameter	Description
Proxy Fallback Intvl	<p>Sets the delay after which the phone retries from the highest priority proxy (or outbound proxy) after it has failed over to a lower priority server.</p> <p>The phone should have the primary and backup proxy server list from a DNS SRV record lookup on the server name. It needs to know the proxy priority; otherwise, it does not retry.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="784 600 1271 653">&lt;Proxy_Fallback_Intvl_1_ua="na"&gt;3600&lt;/Proxy_Fallback_Intvl_1_&gt;</pre> </li> <li>In the phone web page, enter a value in seconds to set the duration in seconds after which the phone retries.</li> </ul> <p>Valid values: Numeric. The range is from 0 seconds to 65535 seconds. Default: 3600 seconds</p>
Proxy Redundancy Method	<p>The phone creates an internal list of proxies returned in the DNS SRV records.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="784 1026 1336 1079">&lt;Proxy_Redundancy_Method_1_ua="na"&gt;Normal&lt;/Proxy_Redundancy_Method_1_&gt;</pre> </li> <li>In the phone web page, select <b>Normal</b> and <b>Based on SRV Port</b>.</li> </ul> <p>If you set to <b>Normal</b>, the list contains proxies ranked by weight and priority.</p> <p>If you set to <b>Based on SRV Port</b>, the phone uses normal, then inspects the port number based on the first-listed proxy port.</p> <p>Valid values: Normal Based on SRV Port Default: Normal</p>
Dual Registration	<p>Controls both the dual registration and the fast fall back feature.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="784 1549 1482 1577">&lt;Dual_Registration_1_ua="na"&gt;No&lt;/Dual_Registration_1_&gt;</pre> </li> <li>In the phone web page, set to <b>Yes</b> to enable the Dual registration/Fast Fall back feature. To enable the feature you must also configure the alternate proxy/alternate outbound proxy fields in the Proxy and Registration section.</li> </ul> <p>Valid values: Yes and No Default: No</p>

Parameter	Description
Auto Register When Failover	<p>Controls the fallback duration.</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="824 428 1386 483">&lt;Auto_Register_When_Failover_1_ua="na"&gt;Yes&lt;/Auto_Register_When_Failover_1_&gt;</pre> </li> <li>In the phone web page, If set to No, the fallback happens immediately and automatically. If the Proxy Fallback Intvl is exceeded, all the new SIP messages go to the primary proxy. <p>If set to Yes, the fallback happens only when current registration expires, which means only a REGISTER message can trigger fallback.</p> <p>For example, when the value for Register Expires is 3600 seconds and Proxy Fallback Intvl is 600 seconds, the fallback is triggered 3600 seconds later and not 600 seconds later. When the value for Register Expires is 600 seconds and Proxy Fallback Intvl is 1000 seconds, the fallback is triggered at 1200 seconds. After successfully registering back to primary server, all the SIP messages go to primary server.</p> <p>Valid values: Yes and No</p> <p>Default: Yes</p> </li> </ul>
TLS Name Validate	<p>This field works only when <b>SIP Transport</b> is set to <b>TLS</b> for the phone line.</p> <p>Specifies whether hostname verification is required when the phone line uses SIP over TLS. The options are:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="824 1283 1523 1308">&lt;TLS_Name_Validate_1_ua="na"&gt;Yes&lt;/TLS_Name_Validate_1_&gt;</pre> </li> <li>In the phone web page, select <b>Yes</b> when hostname verification is required. <p>Select <b>No</b> to bypass the hostname verification.</p> <p>Valid values: Yes and No</p> <p>Default: Yes</p> </li> </ul>

## Configure the Subscriber Information Parameters

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

## Procedure

- 
- Step 1** Select **Voice > Ext(n)**, where n is an extension number.
- Step 2** In the **Subscriber Information** section, set the parameter values as described in the [Subscriber Information Parameters, on page 386](#) table.
- Step 3** Click **Submit All Changes**.
- 

## Subscriber Information Parameters

The following table defines the function and usage of the parameters in the RTP Parameters section under the SIP tab in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file with XML(cfg.xml) code to configure a parameter.

**Table 61: Subscriber Information**

Parameter	Description
Display Name	<p>Name displayed as the caller ID.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:           <pre>&lt;Display_Name_1_ ua="na"/&gt;</pre> </li> <li>In the phone web page, enter a name that represents the caller ID.</li> </ul>
User ID	<p>Extension number for this line.</p> <p>When you need to refer to this user ID in another setting, for example, the short name for a line key, use the \$USER macro variable.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:           <pre>&lt;User_ID_1_ ua="na"&gt;7001&lt;/User_ID_1_&gt;</pre> </li> <li>In the phone web page, enter an extension number</li> </ul>

Parameter	Description
Password	<p>Password for this line.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="1013 474 1463 527">&lt;Password_1_ua="na"&gt;*****&lt;/Password_1_&gt;</pre> </li> <li>In the phone web page, enter a value to add password for the line.</li> </ul> <p>Default: Blank (no password required)</p>
Auth ID	<p>Authentication ID for SIP authentication.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="1013 867 1284 890">&lt;Auth_ID_1_ua="na"/&gt;</pre> </li> <li>In the phone web page, enter a value for an authentication ID.</li> </ul> <p>Default: Blank</p>
Reversed Auth Realm	<p>The IP address for an authentication realm other than the proxy IP address.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="1013 1262 1422 1314">&lt;Reversed_Auth_Realm_1_ua="na"&gt;&lt;/Reversed_Auth_Realm_1_&gt;</pre> <p>The parameter for extension 1 appears as defined in the phone configuration file.</p> </li> <li>In the phone web page, enter proxy IP address.</li> </ul> <p>Default: Blank. The proxy IP address is used as the authentication realm.</p>

Parameter	Description
SIP URI	<p>The parameter by which the user agent will identify itself for this line. If this field is blank, the actual URI used in the SIP signaling should be automatically formed as:</p> <p>sip:UserName@Domain</p> <p>where UserName is the username given for this line in the User ID, and Domain is the domain given for this profile in the User Agent Domain. If the User Agent Domain is an empty string, then the IP address of the phone should be used for the domain.</p> <p>If the URI field is not empty, but if a SIP or SIPS URI contains no @ character, the actual URI used in the SIP signaling should be automatically formed by appending this parameter with an @ character followed by the IP address of the device.</p>

## Set Up Your Phone to Use OPUS Codec Narrowband

To improve bandwidth in your network, you can set up your phones to use the narrowband OPUS codec. The narrowband codec won't conflict with the wideband codec.

### Before you begin

[Access the Phone Web Interface, on page 100](#)

### Procedure

- 
- Step 1** Select **Voice > Ext <n>** where (n) is the number of the extension to configure.
- Step 2** In the **SIP Settings** section, set **Use low-bandwidth OPUS** to **Yes**.
- Step 3** Click **Submit All Changes**.
- 

## NAT Transversal with Phones

Network Address Translation (NAT) allows multiple devices to share a single, public, routable, IP address to establish connections over the Internet. NAT is present in many broadband access devices to translate public and private IP addresses. For VoIP to coexist with NAT, NAT traversal is required.

Not all service providers provide NAT traversal. If your service provider does not provide NAT traversal, you have several options:

- **NAT Mapping with Session Border Controller:** We recommend that you choose a service provider that supports NAT mapping through a Session Border Controller. With NAT mapping provided by the service provider, you have more choices in selecting a router.

- **NAT Mapping with SIP-ALG Router:** NAT mapping can be achieved by using a router that has a SIP Application Layer Gateway (ALG). By using a SIP-ALG router, you have more choices in selecting an service provider.
- **NAT Mapping with a Static IP Address:** NAT mapping with an external (public) static IP address can be achieved to ensure interoperability with the service provider. The NAT mechanism used in the router must be symmetric. For more information, see [Determine Symmetric or Asymmetric NAT, on page 396](#).  
Use NAT mapping only if the service provider network does not provide a Session Border Controller functionality. For more information on how to configure NAT mapping with a static IP, see [Configure NAT Mapping with the Static IP Address , on page 391](#).
- **NAT Mapping with STUN:** If the service provider network does not provide a Session Border Controller functionality and if the other requirements are met, it is possible to use Session Traversal Utilities for NAT (STUN) to discover the NAT mapping. For information on how to configure NAT mapping with STUN, see [Configure NAT mapping with STUN, on page 395](#).

## Enable NAT Mapping

You must enable NAT mapping to set NAT parameters.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

---

- Step 1** Select **Voice > Ext(n)**.
  - Step 2** Set up the fields as described in [NAT Mapping Parameters, on page 390](#).
  - Step 3** Click **Submit All Changes**.
-

## NAT Mapping Parameters

The following table defines the function and usage of NAT Mapping parameters in the NAT Settings section under the Voice>Ext(n) tab in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file with XML(cfg.xml) code to configure a parameter.

**Table 62: NAT Mapping Parameters**

Parameter	Description
NAT Mapping Enable	<p>To use externally mapped IP addresses and SIP/ RTP ports in SIP messages, select yes. Otherwise, select no.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;NAT_Mapping_Enable_1_ua="na"&gt;Yes&lt;/NAT_Mapping_Enable_1_&gt;</pre> </li> <li>In the phone web page, set the parameter to <b>Yes</b>.</li> </ul> <p>Allowed values: Yes No Default: No</p>
NAT Keep Alive Enable	<p>To send the configured NAT keep alive message periodically, select yes. Otherwise, select no.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;NAT_Keep_Alive_Enable_1_ua="na"&gt;Yes&lt;/NAT_Keep_Alive_Enable_1_&gt;</pre> </li> <li>In the phone web page, set the parameter to <b>Yes</b>.</li> </ul> <p>Allowed values: Yes No Default: No</p>



Parameter	Description
NAT Keep Alive Msg	<p>Enter the keep alive message that should be sent periodically to maintain the current NAT mapping.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;NAT_Keep_Alive_Msg_1_ ua="na"&gt;\$NOTIFY&lt;/NAT_Keep_Alive_Msg_1_&gt;</pre> </li> <li>In the phone web page, set the parameter to <b>\$NOTIFY</b> or to <b>\$REGISTER</b>.</li> </ul> <p>If the value is \$NOTIFY, a NOTIFY message is sent. If the value is \$REGISTER, a REGISTER message without contact is sent.</p> <p>Allowed values: \$NOTIFY and \$REGISTER.</p> <p>Default: \$NOTIFY</p>
NAT Keep Alive Dest	<p>Destination that should receive NAT keep alive messages.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;NAT_Keep_Alive_Dest_1_ ua="na"&gt;\$PROXY&lt;/NAT_Keep_Alive_Dest_1_&gt;</pre> </li> <li>In the phone web page, set the parameter to <b>\$PROXY</b> or specify a proxy server.</li> </ul> <p>If the value is \$PROXY, the messages are sent to the current or outbound proxy.</p> <p>Allowed values: \$PROXY or a proxy server IP address</p> <p>Default: \$PROXY</p>

## Configure NAT Mapping with the Static IP Address

You can configure NAT mapping on the phone to ensure interoperability with the service provider.

### Before you begin

- Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).
- You must have an external (public) IP address that is static.
- The NAT mechanism used in the router must be symmetric.

## Procedure

- 
- Step 1** Select **Voice > SIP**.
- Step 2** In the **NAT Support Parameters** section, set the parameters as described in the [NAT Mapping with Static IP Parameters, on page 392](#) table.
- Step 3** Click the **Ext(n)** tab.
- Step 4** In the **NAT Settings** section, set the parameters as described in the [NAT Mapping from Ext Tab with Static IP Parameters](#) table.
- Step 5** Click **Submit All Changes**.
- 

## What to do next

Configure the firewall settings on your router to allow SIP traffic.

## NAT Mapping with Static IP Parameters

The following table defines the function and usage of NAT mapping with Static IP parameters in the NAT Support Parameters section under the Voice>SIP tab in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file with XML(cfg.xml) code to configure a parameter.

*Table 63: NAT Mapping with Static IP Parameters*

Parameter	Description
Handle VIA received	<p>Enables the phone to process the received parameter in the VIA header.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;Handle_VIA_received ua="na"&gt;Yes&lt;/Handle_VIA_received&gt;</pre> </li> <li>In the phone web page, set to <b>Yes</b>.</li> </ul> <p>Default: No</p>
Handle VIA rport	<p>Enables the phone to process the rport parameter in the VIA header.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;Handle_VIA_rport ua="na"&gt;Yes&lt;/Handle_VIA_rport&gt;</pre> </li> <li>In the phone web page, set to <b>Yes</b>.</li> </ul> <p>Default: No</p>

Parameter	Description
Insert VIA received	<p>Enables to insert the received parameter into the VIA header of SIP responses if the received-from IP and VIA sent-by IP values differ.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;Insert_VIA_received ua="na"&gt;Yes&lt;/Insert_VIA_received&gt;</pre> </li> <li>In the phone web page, set to <b>Yes</b>.</li> </ul> <p>Default: No</p>
Insert VIA rport	<p>Enables to insert the rport parameter into the VIA header of SIP responses if the received-from IP and VIA sent-by IP values differ.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;Insert_VIA_rport ua="na"&gt;Yes&lt;/Insert_VIA_rport&gt;</pre> </li> <li>In the phone web page, set to <b>Yes</b>.</li> </ul> <p>Default: No</p>
Substitute VIA Addr	<p>Enables the user to use NAT-mapped IP:port values in the VIA header.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;Substitute_VIA_Addr ua="na"&gt;Yes&lt;/Substitute_VIA_Addr&gt;</pre> </li> <li>In the phone web page, set to <b>Yes</b>.</li> </ul> <p>Default: No</p>
Send Resp To Src Port	<p>Enables to send responses to the request source port instead of the VIA sent-by port.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;Send_Resp_To_Src_Port ua="na"&gt;Yes&lt;/Send_Resp_To_Src_Port&gt;</pre> </li> <li>In the phone web page, set to <b>Yes</b>.</li> </ul> <p>Default: No</p>

Parameter	Description
NAT Keep Alive Intvl	<p>Interval between NAT-mapping keep alive messages.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;NAT_Keep_Alive_Intvl ua="na"&gt;15&lt;/NAT_Keep_Alive_Intvl&gt;</pre> </li> <li>In the phone web page, enter an appropriate value.</li> </ul> <p>Allowed values: Numeric ranges from 0 through 65535</p> <p>Default: 15</p>
EXT IP	<p>External IP address to substitute for the actual IP address of phone in all outgoing SIP messages. If 0.0.0.0 is specified, no IP address substitution is performed.</p> <p>If this parameter is specified, phone assumes this IP address when generating SIP messages and SDP (if NAT Mapping is enabled for that line).</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;EXT_IP ua="na"&gt;10.23.31.43&lt;/EXT_IP&gt;</pre> </li> <li>In the phone web page, enter an external static IP address.</li> </ul> <p>Default: Blank</p>

The following table defines the function and usage of NAT mapping with Static IP parameters in the NAT Support Parameters section under the Voice>Ext tab in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file with XML(cfg.xml) code to configure a parameter.

**Table 64: NAT Mapping from Ext Tab**

Parameter	Description
NAT Mapping Enable	<p>Controls the use of externally mapped IP addresses and SIP/ RTP ports in SIP messages.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;NAT_Mapping_Enable_1_ ua="na"&gt;Yes&lt;/NAT_Mapping_Enable_1_&gt;</pre> </li> <li>In the phone web page, set to <b>Yes</b> to use externally mapped IP addresses.</li> </ul> <p>Allowed values: Yes and No.</p> <p>Default: No</p>

Parameter	Description
NAT Keep Alive Enable (Optional)	<p>Configured NAT keep alive message periodically.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;NAT_Keep_Alive_Enable_1_ua="na"&gt;Yes&lt;/NAT_Keep_Alive_Enable_1_&gt;</pre> </li> <li>In the phone web page, set to <b>Yes</b> to configure periodic NAT keep alive messages.</li> </ul> <p><b>Note</b> The service provider might require the phone to send NAT keep alive messages to keep the NAT ports open.</p> <p>Check with your service provider to determine the requirements.</p> <p>Allowed values: Yes and No.</p> <p>Default: No</p>

## Configure NAT mapping with STUN

If the service provider network does not provide a Session Border Controller functionality and if the other requirements are met, it is possible to use Session Traversal Utilities for NAT (STUN) to discover the NAT mapping. The STUN protocol allows applications operating behind a network address translator (NAT) to discover the presence of the network address translator and to obtain the mapped (public) IP address (NAT addresses) and the port number that the NAT has allocated for the User Datagram Protocol (UDP) connections to remote hosts. The protocol requires assistance from a third-party network server (STUN server) located on the opposing (public) side of the NAT, usually the public Internet. This option is considered a last resort and should be used only if the other methods are not available. To use STUN:

- The router must use asymmetric NAT. See [Determine Symmetric or Asymmetric NAT, on page 396](#).
- A computer running STUN server software is available on the network. You can also use a public STUN server or set up your own STUN server.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

- 
- Step 1** Select **Voice > SIP**.
- Step 2** In the **NAT Support Parameters** section, set the **Handle VIA received**, **Insert VIA received**, **Substitute VIA Addr**, **Handle VIA rport**, **Insert VIA rport**, and **Send Resp To Src Port** parameters as described in the [NAT Mapping with Static IP Parameters, on page 392](#) table.
- Step 3** Set the parameters as described in the [NAT Mapping with STUN Parameters](#) table.
- Step 4** Click the **Ext(n)** tab.
- Step 5** In the **NAT Settings** section, set the parameters as described in the [NAT Mapping from Ext Tab with Static IP Parameters](#) table.

**Step 6** Click **Submit All Changes**.**What to do next**

Configure the firewall settings on your router to allow SIP traffic.

**NAT Mapping with STUN Parameters**

The following table defines the function and usage of NAT mapping with STUN parameters in the NAT Support Parameters section under the Voice>SIP tab in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file with XML(cfg.xml) code to configure a parameter.

*Table 65: NAT Mapping with STUN Parameters*

Parameter	Description
STUN Enable	<p>Enables the use of STUN to discover NAT mapping.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;STUN_Enable ua="na"&gt;Yes&lt;/STUN_Enable&gt;</pre> </li> <li>In the phone web page, set to <b>Yes</b> to enable the feature.</li> </ul> <p>Allowed values: Yes and No. Default: No</p>
STUN Server	<p>IP address or fully-qualified domain name of the STUN server to contact for NAT mapping discovery. You can use a public STUN server or set up your own STUN server.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:  <pre>&lt;STUN_Server ua="na"/&gt;</pre> </li> <li>In the phone web page, enter an IP address or fully-qualified domain name of the STUN server.</li> </ul> <p>Allowed values: Default: Blank</p>

**Determine Symmetric or Asymmetric NAT**

STUN does not work on routers with symmetric NAT. With symmetric NAT, IP addresses are mapped from one internal IP address and port to one external, routable destination IP address and port. If another packet is sent from the same source IP address and port to a different destination, a different IP address and port number

combination is used. This method is restrictive because an external host can send a packet to a particular port on the internal host only if the internal host first sent a packet from that port to the external host.

This procedure assumes that a syslog server is configured and is ready to receive syslog messages.

To Determine Whether the Router Uses Symmetric or Asymmetric NAT:

#### Before you begin

- Verify that the firewall is not running on your PC. (It can block the syslog port.) By default, the syslog port is 514.
- Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

#### Procedure

---

- Step 1** Select **Voice > System** and navigate to **Optional Network Configuration** section.
- Step 2** Enter the IP address for the **Syslog Server**, if the port number is anything other than the default, 514. It is not necessary to include the port number if it is the default.
- The address and port number must be reachable from the Cisco IP phone. The port number appears on the output log file name. The default output file is `syslog.514.log` (if port number was not specified).
- Step 3** Set the **Debug Level** to **Error, Notice, or Debug**.
- Step 4** To capture SIP signaling messages, click the **Ext** tab and navigate to **SIP Settings**. Set the **SIP Debug Option** to **Full**.
- Step 5** To collect information about what type of NAT your router uses click the **SIP** tab and navigate to **NAT Support Parameters**.
- Step 6** Click **Voice > SIP** and navigate to **NAT Support Parameters**.
- Step 7** Set **STUN Test Enable** to **Yes**.
- Step 8** Determine the type of NAT by viewing the debug messages in the log file. If the messages indicate that the device is using symmetric NAT, you cannot use STUN.
- Step 9** Click **Submit All Changes**.
- 

## Dial Plan

### Dial Plan Overview

Dial plans determine how digits are interpreted and transmitted. They also determine whether the dialed number is accepted or rejected. You can use a dial plan to facilitate dialing or to block certain types of calls such as long distance or international.

Use the phone web user interface to configure dial plans on the IP phone.

This section includes information that you must understand about dial plans, and procedures to configure your own dial plans.

The Cisco IP Phone has various levels of dial plans and processes the digits sequence.

When a user presses the speaker button on the phone, the following sequence of events begins:

1. The phone begins to collect the dialed digits. The interdigit timer starts to track the time that elapses between digits.
2. If the interdigit timer value is reached, or if another terminating event occurs, the phone compares the dialed digits with the IP phone dial plan. This dial plan is configured in the phone web user interface in **Voice > Ext(n)** under the **Dial Plan** section.

## Digit Sequences

A dial plan contains a series of digit sequences, separated by the | character. The entire collection of sequences is enclosed within parentheses. Each digit sequence within the dial plan consists of a series of elements that are individually matched to the keys that the user presses.

White space is ignored, but can be used for readability.

Digit Sequence	Function
0 1 2 3 4 5 6 7 8 9 0 * #	Characters that represent a key that the user must press on the phone keypad.
x	Any character on the phone keypad.
[sequence]	<p>Characters within square brackets create a list of accepted key presses. The user can press any one of the keys in the list.</p> <p>A numeric range, for example, [2-9] allows a user to press any one digit from 2 through 9.</p> <p>A numeric range can include other characters. For example, [35-8*] allows a user to press 3, 5, 6, 7, 8, or *.</p>
. (period)	A period indicates element repetition. The dial plan accepts 0 or more entries of the digit. For example, 01. allows users to enter 0, 01, 011, 0111, and so forth.
<dialed:substituted>	<p>This format indicates that certain <i>dialed</i> digits are replaced by the <i>substituted</i> characters when the sequence is transmitted. The <i>dialed</i> digits can be zero to 9. For example:</p> <p>&lt;8:1650&gt;xxxxxxx</p> <p>When the user presses 8 followed by a seven-digit number, the system automatically replaces the dialed 8 with the sequence 1650. If the user dials <b>85550112</b>, the system transmits <b>1650550112</b>.</p> <p>If the <i>dialed</i> parameter is empty and there is a value in the <i>substituted</i> field, no digits are replaced and the <i>substituted</i> value is always prepended to the transmitted string. For example:</p> <p>&lt;:1&gt;xxxxxxxxxxx</p> <p>When the user dials <b>972550112</b>, the number 1 is added at the beginning of the sequence; the system transmits <b>1972550112</b>.</p>



Digit Sequence	Function
, (comma)	An intersequence tone played (and placed) between digits plays an outside line dial tone. For example:  9, 1xxxxxxxxxx  An outside line dial tone plays after the user presses 9. The tone continues until the user presses 1.
! (exclamation point)	Prohibits a dial sequence pattern. For example:  1900xxxxxxxx!  Rejects any 11-digit sequence that begins with 1900.
*xx	Allows a user to enter a 2-digit star code.
S0 or L0	For Interdigit Timer Master Override, enter S0 to reduce the short interdigit timer to 0 seconds, or enter L0 to reduce the long interdigit timer to 0 seconds.
P	To pause, enter P, the number of seconds to pause, and a space. This feature is typically used for implementation of a hotline and warm line, with a 0 delay for the hot line, and a nonzero delay for a warm line. For example:  P5  A pause of 5 seconds is introduced.

## Digit Sequence Examples

The following examples show digit sequences that you can enter in a dial plan.

In a complete dial plan entry, sequences are separated by a pipe character (|), and the entire set of sequences is enclosed within parentheses:

```
( [1-8]xx | 9, xxxxxxxx | 9, <:1>[2-9]xxxxxxxxxx | 8, <:1212>xxxxxxxx | 9, 1 [2-9] xxxxxxxxxxxx | 9, 1 900 xxxxxxxx ! | 9, 011xxxxxxx. | 0 | [49]11 )
```

- Extensions on your system:

```
( [1-8]xx | 9, xxxxxxxx | 9, <:1>[2-9]xxxxxxxxxx | 8, <:1212>xxxxxxxx | 9, 1 [2-9] xxxxxxxxxxxx | 9, 1 900 xxxxxxxx ! | 9, 011xxxxxxx. | 0 | [49]11 )
```

[1-8]xx Allows a user to dial any three-digit number that starts with the digits 1 to 8. If your system uses four-digit extensions, enter the following string: [1-8]xxx

- Local dialing with seven-digit number:

```
( [1-8]xx | 9, xxxxxxxx | 9, <:1>[2-9]xxxxxxxxxx | 8, <:1212>xxxxxxxx | 9, 1 [2-9] xxxxxxxxxxxx | 9, 1 900 xxxxxxxx ! | 9, 011xxxxxxx. | 0 | [49]111 )
```

9, xxxxxxxx After a user presses 9, an external dial tone sounds. The user can enter any seven-digit number, as in a local call.

- Local dialing with 3-digit area code and a 7-digit local number:

```
( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxx
| 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )
```

9, <:1>[2-9]xxxxxxxx This example is useful where a local area code is required. After a user presses 9, an external dial tone sounds. The user must enter a 10-digit number that begins with a digit 2 through 9. The system automatically inserts the 1 prefix before it transmits the number to the carrier.

- Local dialing with an automatically inserted 3-digit area code:

```
( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxx
| 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )
```

8, <:1212>xxxxxxx This example is useful where a local area code is required by the carrier but most calls go to one area code. After the user presses 8, an external dial tone sounds. The user can enter any seven-digit number. The system automatically inserts the 1 prefix and the 212 area code before it transmits the number to the carrier.

- U.S. long-distance dialing:

```
( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxx
| 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )
```

9, 1 [2-9] xxxxxxxx After the user presses 9, an external dial tone sounds. The user can enter any 11-digit number that starts with 1 and is followed by a digit 2 through 9.

- Blocked number:

```
( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxx
| 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )
```

9, 1 900 xxxxxxx ! This digit sequence is useful if you want to prevent users from dialing numbers that are associated with high tolls or inappropriate content, such as 1-900 numbers in the U.S. After the user presses 9, an external dial tone sounds. If the user enters an 11-digit number that starts with the digits 1900, the call is rejected.

- U.S. international dialing:

```
( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxx
| 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )
```

9, 011xxxxxx After the user presses 9, an external dial tone sounds. The user can enter any number that starts with 011, as in an international call from the U.S.

- Informational numbers:

```
( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxx
| 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )
```

0 | [49]11 This example includes two-digit sequences, separated by the pipe character. The first sequence allows a user to dial 0 for an operator. The second sequence allows the user to enter 411 for local information or 911 for emergency services.

## Acceptance and Transmission of the Dialed Digits

When a user dials a series of digits, each sequence in the dial plan is tested as a possible match. The matching sequences form a set of candidate digit sequences. As the user enters more digits, the set of candidates diminishes until only one or none is valid. When a terminating event occurs, the IP PBX either accepts the user-dialed sequence and initiates a call, or else rejects the sequence as invalid. The user hears the reorder (fast busy) tone if the dialed sequence is invalid.

The following table explains how terminating events are processed.

Terminating Event	Processing
Dialed digits have not matched any sequence in the dial plan.	The number is rejected.
Dialed digits exactly match one sequence in the dial plan.	If the dial plan allows the sequence, the number is accepted and is transmitted according to the dial plan.  If the dial plan blocks the sequence, the number is rejected.
A timeout occurs.	The number is rejected if the dialed digits are not matched to a digit sequence in the dial plan within the time that the applicable interdigit timer specifies.  The Interdigit Long Timer applies when the dialed digits do not match any digit sequence in the dial plan.  Default: 10 seconds.  The Interdigit Short Timer applies when the dialed digits match one or more candidate sequences in the dial plan. Default: 3 seconds.
A user presses the # key or the dial softkey on the IP phone screen.	If the sequence is complete and is allowed by the dial plan, the number is accepted and is transmitted according to the dial plan.  If the sequence is incomplete or is blocked by the dial plan, the number is rejected.

### Dial Plan Timer (Off-Hook Timer)

You can think of the Dial Plan Timer as the off-hook timer. This timer starts when the phone goes off hook. If no digits are dialed within the specified number of seconds, the timer expires and the null entry is evaluated. Unless you have a special dial plan string to allow a null entry, the call is rejected.



**Note** The timer before a number is dialed is whichever shorter of the dial plan default timer and the dial tone timer set in the **Dial Tone** field on the **Regional** tab.

#### Syntax for the Dial Plan Timer

**SYNTAX:** (P<:n> | dial plan)

- **s**: The number of seconds; The timer before a number is dialed is whichever shorter of the dial plan default timer and the dial tone timer set in the **Dial Tone** field. With the timer set to 0 seconds, the call transmits automatically to the specified extension when the phone goes off hook.
- **n**: (optional): The number to transmit automatically when the timer expires; you can enter an extension number or a DID number. No wildcard characters are allowed because the number is transmitted as shown. If you omit the number substitution, <n>, the user hears a reorder (fast busy) tone after the specified number of seconds.

## Examples for the Dial Plan Timer



**Note** The actual timer before a number is dialed is whichever shorter of the dial plan default timer and the dial tone timer set in the **Dial Tone** field. In the following examples, the dial tone timer is assumed to be longer than the dial plan timer.

Allow more time for users to start dialing after taking a phone off hook:

```
(P9 | (9,8<:1408>[2-9]xxxxxx | 9,8,1[2-9]xxxxxxxxxx | 9,8,011xx. | 9,8,xx.[1-8]xx)
```

P9 means that after taking a phone off hook, a user has 9 seconds to begin dialing. If no digits are pressed within 9 seconds, the user hears a reorder (fast busy) tone. By setting a longer timer, you allow more time for users to enter digits.

To create a hotline for all sequences on the System Dial Plan:

```
(P9<:23> | (9,8<:1408>[2-9]xxxxxx | 9,8,1[2-9]xxxxxxxxxx | 9,8,011xx. | 9,8,xx.[1-8]xx)
```

P9<:23> means that after taking the phone off hook, a user has 9 seconds to begin dialing. If no digits are pressed within 9 seconds, the call is transmitted automatically to extension 23.

To create a hotline on a line button for an extension:

```
(P0 <:1000>)
```

With the timer set to 0 seconds, the call is transmitted automatically to the specified extension when the phone goes off hook. Enter this sequence in the Phone Dial Plan for Ext 2 or higher on a client phone.

## Interdigit Long Timer (Incomplete Entry Timer)

You can think of this timer as the incomplete entry timer. This timer measures the interval between dialed digits. It applies as long as the dialed digits do not match any digit sequences in the dial plan. Unless the user enters another digit within the specified number of seconds, the entry is evaluated as incomplete, and the call is rejected. The default value is 10 seconds.

This section explains how to edit a timer as part of a dial plan. Alternatively, you can modify the Control Timer that controls the default interdigit timers for all calls.

### Syntax for the Interdigit Long Timer

**SYNTAX:** L:s, (dial plan)

- **s**: The number of seconds; if no number is entered after L:, the default timer is 5 seconds. With the timer set to 0 seconds, the call is transmitted automatically to the specified extension when the phone goes off hook.
- Note that the timer sequence appears to the left of the initial parenthesis for the dial plan.

### Example for the Interdigit Long Timer

```
L:15, (9,8<:1408>[2-9]xxxxxx | 9,8,1[2-9]xxxxxxxxxx | 9,8,011xx. | 9,8,xx.|[1-8]xx)
```

L:15 means that this dial plan allows the user to pause for up to 15 seconds between digits before the Interdigit Long Timer expires. This setting is especially helpful to users such as sales people, who are reading the numbers from business cards and other printed materials while dialing.

### Interdigit Short Timer (Complete Entry Timer)

You can think of this timer as the complete entry timer. This timer measures the interval between dialed digits. The timer applies when the dialed digits match at least one digit sequence in the dial plan. Unless the user enters another digit within the specified number of seconds, the entry is evaluated. If the entry is valid, the call proceeds. If the entry is invalid, the call is rejected.

Default: 3 seconds.

### Syntax for the Interdigit Short Timer

**SYNTAX 1:** S:s, (dial plan)

Use this syntax to apply the new setting to the entire dial plan within the parentheses.

**SYNTAX 2:** *sequence* Ss

Use this syntax to apply the new setting to a particular dialing sequence.

**s**: The number of seconds; if no number is entered after S, the default timer of 5 seconds applies.

### Examples for the Interdigit Short Timer

To set the timer for the entire dial plan:

```
S:6, (9,8<:1408>[2-9]xxxxxx | 9,8,1[2-9]xxxxxxxxxx | 9,8,011xx. | 9,8,xx.|[1-8]xx)
```

S:6 means that while the user enters a number with the phone off hook, the user can pause for up to 15 seconds between digits before the Interdigit Short Timer expires. This setting is especially helpful to users such as sales people, who are reading the numbers from business cards and other printed materials while dialing.

Set an instant timer for a particular sequence within the dial plan:

```
(9,8<:1408>[2-9]xxxxxx | 9,8,1[2-9]xxxxxxxxxxS0 | 9,8,011xx. | 9,8,xx.|[1-8]xx)
```

9,8,1[2-9]xxxxxxxxxxS0 means that with the timer set to 0, the call is transmitted automatically when the user dials the final digit in the sequence.

## Edit the Dial Plan on the IP Phone



**Note** You can edit the dial plan in the XML configuration file. Locate the `Dial_Plan_n` parameter in the XML configuration file, where `n` denotes the extension number. Edit the value of this parameter. The value must be specified in the same format as in the **Dial Plan** field on the phone administration web page, described below.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

**Step 1** Select **Voice > Ext(n)**, where `n` is an extension number.

**Step 2** Scroll to the **Dial Plan** section.

**Step 3** Enter the digit sequences in the **Dial Plan** field.

The default (US-based) systemwide dial plan appears automatically in the field.

**Step 4** You can delete digit sequences, add digit sequences, or replace the entire dial plan with a new dial plan.

Separate each digit sequence with a pipe character, and enclose the entire set of digit sequences within parentheses. Example:

```
(9,8<:1408>[2-9]xxxxxxx | 9,8,1[2-9]xxxxxxxxxxx | 9,8,011xx. | 9,8,xx.|[1-8]xx)
```

**Step 5** Click **Submit All Changes**.

The phone reboots.

**Step 6** Verify that you can successfully complete a call with each digit sequence that you entered in the dial plan.

**Note** If you hear a reorder (fast busy) tone, review your entries and modify the dial plan appropriately.

## Regional Parameters Configuration

### Regional Parameters

In the phone web user interface, use the **Regional** tab to configure regional and local settings, such as control timer values, dictionary server script, language selection, and locale to change localization. The Regional tab includes these sections:

- Call Progress Tones—Displays values of all ringtones.
- Distinctive Ring Patterns—Ring cadence defines the ringing pattern that announces a telephone call.

- Control Timer Values—Displays all values in seconds.
- Vertical Service Activation Codes—Includes Call Back Act Code and Call Back Deact Code.
- Outbound Call Codec Selection Codes—Defines the voice quality.
- Time—Includes local date, local time, time zone, and Daylight Saving Time.
- Language—Includes Dictionary Server Script, Language Selection, and Locale.

## Set the Control Timer Values

If you need to edit a timer setting only for a particular digit sequence or type of call, you can edit the dial plan.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

- 
- |               |                                                                                                                                                                         |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Select <b>Voice &gt; Regional</b> .                                                                                                                                     |
| <b>Step 2</b> | Set the <b>Reorder Delay</b> , <b>Interdigit Long Timer</b> , and <b>Interdigit Short Timer</b> parameters as described in the <b>Control Timer Values (sec)</b> table. |
| <b>Step 3</b> | Click <b>Submit All Changes</b> .                                                                                                                                       |
- 

## Parameters for Control Timer Values (sec)

The following table defines the function and usage of Control Timer Values parameters in the Control Timer Values(s) Parameters section under the Voice>Regional tab in the phone web interface. It also defines the

syntax of the string that is added in the phone configuration file with XML(cfg.xml) code to configure a parameter.

**Table 66: Parameters for Control Timer Values (sec)**

Parameter	Description
Reorder Delay	<p>Delay after far end hangs up before reorder (busy) tone is played.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:           <pre data-bbox="976 646 1321 701">&lt;Reorder_Delay ua="na"&gt;255&lt;/Reorder_Delay&gt;</pre> </li> <li>In the phone web page, set a value in seconds ranges from 0-255 secs.</li> </ul> <p>0 = plays immediately, inf = never plays. Set to 255 to return the phone immediately to on-hook status and to not play the tone.</p> <p>Allowed values: 0–255 seconds</p> <p>Default: 255</p>
Interdigit Long Timer	<p>Long timeout between entering digits when dialing. The interdigit timer values are used as defaults when dialing. The Interdigit_Long_Timer is used after any one digit, if all valid matching sequences in the dial plan are incomplete as dialed.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format:           <pre data-bbox="976 1329 1409 1383">&lt;Interdigit_Long_Timer ua="na"&gt;10&lt;/Interdigit_Long_Timer&gt;</pre> </li> <li>In the phone web page, set a value in seconds ranges from 0-64 seconds.</li> </ul> <p>Allowed values: 0–64 seconds</p> <p>Default: 10</p>



Parameter	Description
Interdigit Short Timer	<p>Short timeout between entering digits when dialing. The Interdigit_Short_Timer is used after any one digit, if at least one matching sequence is complete as dialed, but more dialed digits would match other as yet incomplete sequences.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre>&lt;Interdigit_Short_Timer ua="na"&gt;3&lt;/Interdigit_Short_Timer&gt;</pre> </li> <li>In the phone web page, set a value in seconds ranges from 0-64 seconds.</li> </ul> <p>Allowed values: 0–64 seconds Default: 3</p>

## Localize Your Cisco IP Phone

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

- 
- Step 1** Select **Voice > Regional**.
  - Step 2** Configure the values in the fields in the **Time** and **Language** sections.
  - Step 3** Click **Submit All Changes**.
- 

## Configure Time and Date on Phone Web Page

You can manually set the time and date on the phone web page.

### Before you begin

[Access the Phone Web Interface, on page 100](#). Review [Time and Date Settings, on page 408](#).

### Procedure

- 
- Step 1** Select **Voice > Regional**.
  - Step 2** In the **Time** section, enter the time and date information.
  - Step 3** Select **Voice > User**.

- Step 4** In the **Supplementary Services**, choose **12h** or **24hr** from the **Time Format** drop down list.  
Default: 12hr
- Step 5** Choose the date format from the **Date Format** drop down list.
- Step 6** Click **Submit All Changes**
- 

## Configure Time and Date on the Phone


You can set the time and date manually on the phone.

### Before you begin

Review the [Time and Date Settings, on page 408](#).

### Procedure

---

- Step 1** Press **Applications** .
- Step 2** Select **Device administration** > **Date/Time**.
- Step 3** Select **Set current time manually**.
- Step 4** Set the date and time in the format requested on the screen:  
**YYYY MM DD HH MM**
- Step 5** Select the **OK** softkey.
- Step 6** Select the **Save** softkey.
- 

## Time and Date Settings

The Cisco IP Phone obtains the time settings in one of two ways:

- **NTP Server**— NTP 24-hour time format takes priority over the time you set using the menu options on the phone or web page.

When the phone boots up, it tries to contact the first Network Time Protocol (NTP) server to get and update the time. The phone periodically synchronizes its time with the NTP server, and between updates, it tracks time with its internal clock. The synchronization period is fixed at 64 seconds.

If you manually enter a time, this setting takes effect for now, but on the next NTP synchronization, the NTP time is displayed.

- **Manual Setup**—You can manually configure the local date and time by using one of the following methods:
  - On the phone web interface
  - On the phone itself

The default format is 12-hour which is overwritten with the 24-hour format as soon as the phone synchronizes with the NTP server.

Table 67: Date and Time Parameters

Parameter	Description
Set Local Date (mm/dd/yyyy)	Sets the local date (mm represents the month and dd represents the day). The year is optional and uses two or four digits. Default: Blank
Set Local Time (HH/mm)	Sets the local time (hh represents hours and mm represents minutes). Seconds are optional. Default: Blank
Time Zone	Selects the number of hours to add to GMT to generate the local time for caller ID generation. Choices are GMT-12:00, GMT-11:00, ..., GMT, GMT+01:00, GMT+02:00, ..., GMT+13:00.  The time of the log messages and status messages are in UTC time and are not affected by the time zone setting. Default: GMT-08:00
Time Offset (HH/mm)	This specifies the offset in 24-hour format from GMT to use for the local system time.  The NTP Server time is expressed in GMT time. The local time is obtained by offsetting the GMT according to the time zone of the region. Default: 00/00
Ignore DHCP Time Offset	When used with some routers that have DHCP with time offset values configured, the IP phone uses the router settings and ignores the IP phone time zone and offset settings. To ignore the router DHCP time offset value, and use the local time zone and offset settings, choose <b>yes</b> for this option. If you choose <b>no</b> , the IP phone uses the router's DHCP time offset value. Default: Yes.

Parameter	Description
Daylight Saving Time Rule	<p>Enter the rule for calculating daylight saving time. This rule is comprised of three fields. Each field is separated by a semicolon (;). Optional values inside brackets [ ] are assumed to be 0 if they are not specified. Midnight is represented by colons. For example, 0:0:0 of the given date.</p> <p>This is the format of the rule: Start = &lt;start-time&gt;; end=&lt;end-time&gt;; save = &lt;save-time&gt;.</p> <p>The &lt;start-time&gt; and &lt;end-time&gt; values specify the start and end dates and times of daylight saving time. Each value is in this format: &lt;month&gt; /&lt;day&gt; / &lt;weekday&gt;[/HH:[mm[:ss]]]</p> <p>The &lt;save-time&gt; value is the number of hours, minutes, and/or seconds to add to the current time during daylight saving time. The &lt;save-time&gt; value can be preceded by a negative (-) sign if subtraction is desired instead of addition. The &lt;save-time&gt; value is in this format: [/[+ -]HH:[mm[:ss]]]</p> <p>The &lt;month&gt; value equals any value in the range 1-12 (January-December).</p> <p>The &lt;day&gt; value equals [+ -] any value in the range 1-31.</p> <p>If &lt;day&gt; is -1, it means the &lt;weekday&gt; on or before the end of the month (in other words the last occurrence of &lt; weekday&gt; in that month).</p>
Daylight Saving Time Rule (continued)	<p>The &lt;weekday&gt; value equals any value in the range 1-7 (Monday-Sunday). It can also equal 0. If the &lt;weekday&gt; value is 0, this means that the date to start or end daylight saving is exactly the date given. In that case, the &lt;day&gt; value must not be negative. If the &lt;weekday&gt; value is not 0 and the &lt;day&gt; value is positive, then daylight saving starts or ends on the &lt;weekday&gt; value on or after the date given. If the &lt;weekday&gt; value is not 0 and the &lt;day&gt; value is negative, then daylight saving starts or ends on the &lt;weekday&gt; value on or before the date given. Where:</p> <ul style="list-style-type: none"> <li>• HH stands for hours (0-23).</li> <li>• mm stands for minutes (0-59).</li> <li>• ss stands for seconds (0-59).</li> </ul> <p>Default: 3/-1/7/2;end=10/-1/7/2;save=1.</p>

Parameter	Description
Daylight Saving Time Enable	Enables Daylight Saving Time. Default: Yes
Time Format	Choose the time format for the phone (12-hour or 24-hour). Default: 12hr
Date Format	Choose the date format for the phone (month/day or day/month). Default: month/day  In the phone configuration XML file (cfg.xml), enter a string in this format:  <pre> &lt;!-- Time --&gt; &lt;Set_Local_Date__mm_dd_yyyy_ua="na"/&gt; &lt;Set_Local_Time__HH_mm_ua="na"/&gt; &lt;Time_Zone ua="na"&gt;GMT-08:00&lt;/Time_Zone&gt; &lt;!-- available options: GMT-12:00 GMT-11:00 GMT-10:00 GMT-09:00  GMT-08:00 GMT-07:00 GMT-06:00 GMT-05:00 GMT-04:00 GMT-03:30  GMT-03:00 GMT-02:00 GMT-01:00 GMT GMT+01:00 GMT+02:00 GMT+03:00  GMT+03:30 GMT+04:00 GMT+04:30 GMT+05:00 GMT+05:30 GMT+05:45  GMT+06:00 GMT+06:30 GMT+07:00 GMT+08:00 GMT+09:00 GMT+09:30  GMT+10:00 GMT+11:00 GMT+12:00 GMT+13:00 GMT+14:00 --&gt; --&gt; &lt;Time_Offset__HH_mm_ua="na"/&gt; &lt;Ignore_DHCP_Time_Offset ua="na"&gt;Yes&lt;/Ignore_DHCP_Time_Offset&gt; &lt;Daylight_Saving_Time_Rule ua="na"&gt;start=3/-1/7/2;end=10/-1/7/2; save=1&lt;/Daylight_Saving_Time_Rule&gt; &lt;Daylight_Saving_Time_Enable ua="na"&gt;Yes&lt;/Daylight_Saving_Time_Enable&gt; &lt;Time_Format ua="na"&gt;12hr&lt;/Time_Format&gt; &lt;!-- available options: 12hr 24hr --&gt; &lt;Date_Format ua="na"&gt;month/day&lt;/Date_Format&gt; &lt;!-- available options: month/day day/month --&gt; </pre>

## Configure Daylight Saving Time

The phone supports automatic adjustment for daylight saving time.



**Note** The time of the log messages and status messages are in UTC time. The time zone setting does not affect them.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

## Procedure

---

- Step 1** Select **Voice > Regional**.
  - Step 2** Set the **Daylight Saving Time Enable** drop-down list box to **Yes**.
  - Step 3** In the **Daylight Saving Time Rule** field, enter the DST rule. This value affects the time stamp on the CallerID.
  - Step 4** Click **Submit All Changes**.
- 

## Daylight Saving Time Examples

The following example configures daylight saving time for the U.S, adding one hour starting at midnight on the second Sunday in March and ending at midnight on the first Sunday in November; add 1 hour (USA, North America):

```
start=3/8/7/02:0:0;end=11/1/7/02:0:0;save=1
```

The following example configures daylight saving time for Finland, starting at midnight on the last Sunday in March and ending at midnight on the last Sunday in October:

```
start=3/-1/7/03:0:0;end=10/-1/7/03:0:0;save=1 (Finland)
```

The following example configures daylight saving time for New Zealand (in version 7.5.1 and higher), starting at midnight on the last Sunday in September and ending at midnight on the first Sunday of April.

```
start=9/-1/7/02:0:0;end=4/1/7/02:0:0;save=1 (New Zealand)
```

The following example configures the daylight saving time starting on the last Monday (on or before April 8) and ending on the first Wednesday (on or after May 8).

```
start=4/-8/1;end=5/8/3;save=1
```

## Phone Display Language

The Cisco IP Phone supports multiple languages for the phone display.

By default, the phone is set up for English. To enable the use of another language, you must set up the dictionary for the language. For some languages, you must also set up the font for the language.

After the setup is complete, you or your users can specify the desired language for the phone display.

### Supported Languages for the Phone Display

On the phone administration web page, go to **Admin Login > Advanced > Voice > Regional**. In the **Language** section, click the **Locale** drop-down list box to see the supported languages for the phone display.

- ar-SA (Arabic)
- bg-BG (Bulgarian)
- ca-ES (Catalan)
- cs-CZ (Czech)
- da-DK (Danish)
- de-DE (German)
- el-GR (Greek)
- en-GB (English-Great Britain)
- en-US (English-United States)
- es-CO (Spanish-Colombia)
- es-ES (Spanish-Spain)
- fi-FI (Finnish)
- fr-CA (French-Canada)
- fr-FR (French)
- he-IL (Hebrew)
- hr-HR (Croatian)
- hu-HU (Hungarian)
- it-IT (Italian)
- ja-JP (Japanese)
- ko-KR (Korean)
- nl-NL (Dutch)
- nn-NO (Norwegian)
- pl-PL (Polish)
- pt-PT (Portuguese)
- ru-RU (Russian)
- sk-SK (Slovak)
- sl-SI (Slovenian)
- sv-SE (Swedish)
- tr-TR (Turkish)
- zh-CN (Chinese)
- zh-HK (Chinese-Hong Kong SAR)

## Set Up Dictionaries and Fonts

Languages other than English require dictionaries. Some languages also require a font.




---

**Note** To enable Latin and Cyrillic languages, you must not add a font file.

---

### Procedure

- 
- Step 1** Download the locale zip file for your firmware version, from [cisco.com](http://cisco.com). Place the file on your server, and unzip the file.
- Dictionaries and fonts for all the supported languages are included in the zip file. Dictionaries are XML scripts. Fonts are standard TTF files.
- Step 2** On the phone administration web page, go to **Admin Login > Advanced > Voice > Regional**. In the **Language** section, specify the necessary parameters and values in the **Dictionary Server Script** field as described below. Use a semicolon (;) to separate multiple parameter and value pairs.
- Specify the location of the dictionary and font files with the `serv` parameter.
- For example: `serv=http://server.example.com/Locales/`

Make sure to include the IP address of the server, the path, and folder name.

Example: `serv=http://10.74.128.101/Locales/`

- For each language that you want to set up, specify a set of parameters as described below.

**Note** In these parameter specifications, *n* denotes a serial number. This number determines the sequential order in which the language options are displayed in the **Settings** menu of the phone. 0 is reserved for US-English, which has a default dictionary. You can use it optionally, to specify your own dictionary.

Use numbers starting with 1 for other languages.

- Specify the language name with the `dn` parameter.

Example for language name for Asian language: `d1=Chinese-Simplified`

Example for language name for German (Latin and Cyrillic): `d2=German`

Example for language name for French (Latin and Cyrillic): `d1=French`

Example for language name for French (Canada) (Latin and Cyrillic) language: `d1=French-Canada`

Example for language name for Hebrew (RTL language): `d1=Hebrew`

Example for language name for Arabic (RTL language): `d1=Arabic`

This name is displayed as a language option in the **Settings** menu of the phone.

- Specify the name of the dictionary file with the `xn` parameter.

Example for Asian language:

Example for French (Latin and Cyrillic) languages:

Example for Arabic (RTL language) language:

Example for French (Canada) language:

Ensure to specify the correct file for the language and phone model that you use.

- If a font is required for the language, specify the name of the font file with the `fn` parameter.

For example:

Make sure to specify the correct file for the language and phone model that you use.

See [Setup for Latin and Cyrillic Languages, on page 414](#) for specific details on setting up Latin languages.

See [Setup for an Asian Language, on page 416](#) for specific details on setting up an Asian language.

See [Setup for RTL Languages, on page 416](#) for specific details on setting up RTL languages.

### Step 3 Click **Submit All Changes**.

## Setup for Latin and Cyrillic Languages

If you use Latin and Cyrillic languages such as French or German, you can configure up to four language options for the phone. List of Latin and Cyrillic languages:



- Bulgarian
- Catalan
- Croatian
- Czech
- Danish
- Dutch
- English (UK)
- Finnish
- French (France)
- French (Canada)
- German
- Greek
- Hungarian
- Italian
- Portuguese (Portugal)
- Norwegian
- Polish
- Russian
- Slovak
- Slovenian
- Spanish (Columbia)
- Spanish (Spain)
- Swedish
- Turkish
- Ukraine

To enable the options, set up a dictionary for each language that you want to include. To enable the language, specify a pair of *dn* and *xn* parameters and values in the **Dictionary Server Script** field, for each language that you want to include.

Example for including French and German:

Example for including French (Canada):

```
serv=http://10.74.128.101/Locales/;dl=French-Canada;x1=fr-CA_78xx_68xx-11.3.6.0006xml;
serv=http://10.74.128.101/Locales/;dl=French-Canada;x1=fr-CA_88xx-11.3.6.0006xml;
```



**Note** In the above examples `http://10.74.128.101/Locales/` is a web folder. The dictionary files are extracted in this web folder and are used in the examples.

To configure this option in the phone configuration XML file (cfg.xml), enter a string in this format:

```
<!-- Language -->
<Dictionary_Server_Script ua="na"serv=http://10.74.10.215/locapi/resync_files/dl=French-Canada;x1=fr-CA_88xx-11.3.6.0006.xml;></Dictionary_Server_Script>

<Language_Selection ua="na">French-Canada</Language_Selection>
<Locale ua="na">fr-CA</Locale>
```

Add values for:

- **Language Selection** Parameter as appropriate

For French: **French**

For French (Canada): **French-Canada**

For German: **German**

- **Locale** parameter list as appropriate

For French: **fr-FR**

For French (Canada): **fr-CA**

For German: **de-DE**

After the successful configuration, the user can see the configured language option on the phone under the **Language** menu. User can access the **Language** menu from **Applications > Device administration**.

### Setup for an Asian Language

If you use an Asian language such as Chinese, Japanese, or Korean, you can only set up one language option for the phone.

You must set up the dictionary and the font for the language. To do this, specify the `d1`, `x1` and `f1` parameters and values in the **Dictionary Server Script** field.

Example for setting up Chinese-Simplified:

### Setup for RTL Languages

If you use a Right-to-Left (RTL) language such as Arabic and Hebrew, you can only set up one language option for the phone.

You must set up the dictionary and the font for the language. To do this, specify the `d1`, `x1`, and `f1` parameters and values in the **Dictionary Server Script** field.

Example for Arabic:

```
serv=http://server.example.com/Locales;d1=Arabic;x1=ar-SA_88xx-11.3.4.xml;f1=ar-SA_88xx-11.3.4.ttf
```

Example for Hebrew:

```
serv=http://server.example.com/Locales;d1=Hebrew;x1=he-IL_88xx-11.3.4.xml;f1=he-IL_88xx-11.3.4.ttf
```

Values for **Language Selection** parameter must be **Arabic** or **Hebrew** as appropriate.

Values for **Locale** parameter must be **ar-SA** for Arabic and **he-IL** for Hebrew.

### Specify a Language for the Phone Display




---

**Note** Your users can select the language on the phone, from **Settings > Device Administration > Language**.

---

#### Before you begin

The dictionaries and fonts required for the language are set up. See [Set Up Dictionaries and Fonts](#), on page 413 for details.

## Procedure

- Step 1** On the phone administration web page, go to **Admin Login > Advanced > Voice > Regional, Language** section. In the **Language Selection** field, specify the value of the appropriate `dn` parameter value from the **Dictionary Server Script** field, for the language of your choice.
- Step 2** Click **Submit All Changes**.

## Vertical Service Activation Codes

Parameter	Description
Call Return Code	This code calls the last caller. Defaults to *69.
Blind Transfer Code	Begins a blind transfer of the current call to the extension specified after the activation code. Defaults to *95.
Cfwd All Act Code	Forwards all calls to the extension specified after the activation code. Defaults to *72.
Cfwd All Deact Code	Cancels call forward of all calls. Defaults to *73.
Cfwd Busy Act Code	Forwards busy calls to the extension specified after the activation code. Defaults to *90.
Cfwd Busy Deact Code	Cancels call forward of busy calls. Defaults to *91.
Cfwd No Ans Act Code	Forwards no-answer calls to the extension specified after the activation code. Defaults to *92.
Cfwd No Ans Deact Code	Cancels call forward of no-answer calls. Defaults to *93.
CW Act Code	Enables call waiting on all calls. Defaults to *56.
CW Deact Code	Disables call waiting on all calls. Defaults to *57.

Parameter	Description
CW Per Call Act Code	Enables call waiting for the next call. Defaults to *71.
CW Per Call Deact Code	Disables call waiting for the next call. Defaults to *70.
Block CID Act Code	Blocks caller ID on all outbound calls. Defaults to *61.
Block CID Deact Code	Removes caller ID blocking on all outbound calls. Defaults to *62.
Block CID Per Call Act Code	Removes caller ID blocking on the next inbound call. Defaults to *81.
Block CID Per Call Deact Code	Removes caller ID blocking on the next inbound call. Defaults to *82.
Block ANC Act Code	Blocks all anonymous calls. Defaults to *77.
Block ANC Deact Code	Removes blocking of all anonymous calls. Defaults to *87.
DND Act Code	Enables the do not disturb feature. Defaults to *78.
DND Deact Code	Disables the do not disturb feature. Defaults to *79.
Secure All Call Act Code	Makes all outbound calls secure. Defaults to *16.
Secure No Call Act Code	Makes all outbound calls not secure. Defaults to *17.
Secure One Call Act Code	Makes a secure call. Default: *18.
Secure One Call Deact Code	Disables secure call feature. Default: *19.
Paging Code	The star code used for paging the other clients in the group. Defaults to *96.

Parameter	Description
Call Park Code	The star code used for parking the current call. Defaults to *68.
Call Pickup Code	The star code used for picking up a ringing call. Defaults to *97.
Call Unpark Code	The star code used for picking up a call from the call park. Defaults to *88.
Group Call Pickup Code	The star code used for picking up a group call. Defaults to *98.
Referral Services Codes	<p>These codes tell the IP phone what to do when the user places the current call on hold and is listening to the second dial tone.</p> <p>One or more *code can be configured into this parameter, such as *98, or *97 *98 *123, and so on. Max total length is 79 chars. This parameter applies when the user places the current call on hold (by Hook Flash) and is listening to second dial tone. Each *code (and the following valid target number according to current dial plan) entered on the second dial-tone triggers the phone to perform a blind transfer to a target number that is prepended by the service *code.</p> <p>For example, after the user dials *98, the IP phone plays a special dial tone called the Prompt Tone while waiting for the user to enter a target number (which is checked according to dial plan as in normal dialing). When a complete number is entered, the phone sends a blind REFER to the holding party with the Refer-To target equals to *98&lt;target_number&gt;. This feature allows the phone to hand off a call to an application server to perform further processing, such as call park.</p> <p>The *codes should not conflict with any of the other vertical service codes internally processed by the IP phone. You can empty the corresponding *code that you do not want the phone to process.</p>

Parameter	Description
Feature Dial Services Codes	<p>These codes tell the phone what to do when the user is listening to the first or second dial tone.</p> <p>One or more *code can be configured into this parameter, such as *72, or *72 *74 *67 *82, and so forth. The maximum total length is 79 characters. This parameter applies when the user has a dial tone (first or second dial tone). Enter *code (and the following target number according to current dial plan) entered at the dial tone triggers the phone to call the target number prepended by the *code. For example, after user dials *72, the phone plays a prompt tone awaiting the user to enter a valid target number. When a complete number is entered, the phone sends a INVITE to *72&lt;target_number&gt; as in a normal call. This feature allows the proxy to process features like call forward (*72) or BLock Caller ID (*67).</p> <p>The *codes should not conflict with any of the other vertical service codes internally processed by the phone. You can empty the corresponding *code that you do not want to the phone to process.</p> <p>You can add a parameter to each *code in Features Dial Services Codes to indicate what tone to play after the *code is entered, such as *72'c' *67'p'. Below are a list of allowed tone parameters (note the use of back quotes surrounding the parameter without spaces)</p> <ul style="list-style-type: none"> <li>• c = C fwd Dial Tone</li> <li>• d = Dial Tone</li> <li>• m = MWI Dial Tone</li> <li>• o = Outside Dial Tone</li> <li>• p = Prompt Dial Tone</li> <li>• s = Second Dial Tone</li> <li>• x = No tones are place, x is any digit not used above</li> </ul> <p>If no tone parameter is specified, the phone plays Prompt tone by default.</p> <p>If the *code is not to be followed by a phone number, such as *73 to cancel call forward, do not include it in this parameter. In that case, simple add that *code in the dial plan and the phone sends INVITE *73@..... as usual when user dials *73.</p>

# Cisco IP Conference Phone 8832 Multiplatform Phones Documentation

Refer to publications that are specific to your language and phone model, and phone firmware release. Navigate from the following documentation URL:

<https://www.cisco.com/c/en/us/support/collaboration-endpoints/ip-phone-8800-series-multiplatform-firmware/tsd-products-support-series-home.html>







## PART **IV**

# Troubleshooting

- [Troubleshooting, on page 425](#)
- [Monitoring Phone Systems, on page 437](#)
- [Maintenance, on page 445](#)





## CHAPTER 17

# Troubleshooting

---

- [Feature Troubleshooting](#), on page 425
- [Phone Display Problems](#), on page 430
- [Report All Phone Issues from Phone Web Page](#), on page 431
- [Report Phone Issues from Webex Control Hub](#), on page 432
- [Factory Reset the Phone from Phone Web Page](#), on page 432
- [Reboot the Phone from the Webex Control Hub](#), on page 433
- [Report a Phone Problem Remotely](#), on page 433
- [Capture Packets](#), on page 434
- [Voice Quality Troubleshooting Tips](#), on page 434
- [Where to Find Additional Information](#), on page 435

## Feature Troubleshooting

Here is troubleshooting information related to some of the phone features.

### ACD Call Information Missing

#### Problem

A call center phone does not see call information during a call.

#### Solution

- Check the phone configuration to determine if **Call Information Enable** is set to yes.
- Check the Broadsoft server configuration to determine if the user's Device Profile is configured with "Support Call Center MIME Type".

### Phone Doesn't Show ACD Softkeys

#### Problem

The phone doesn't display the Agent Sign In or Agent Sign Out softkeys.

**Solution**

- Check Broadsoft server configuration to determine if that user has been configured as a call center agent.
- Enable the programmable softkeys (PSK) and add the ACD softkeys to the softkey list. For more information, see [Customize Display of the Softkeys, on page 271](#).
- Check the phone configuration to determine if **BroadSoft ACD** is set to yes.

## Phone Doesn't Show ACD Agent Availability

**Problem**

The phone doesn't display the Avail or Unavail softkeys for an agent.

**Solution**

1. Check Broadsoft server configuration to determine if that user has been configured as a call center agent.
2. Check the phone configuration to determine if **BroadSoft ACD** is set to yes.
3. Set up the **Agt Status** programmable softkey (PSK) and add the ACD softkey to the softkey list. For more information, see [Customize Display of the Softkeys, on page 271](#).
4. Instruct users to press the **Agt Status** key to display the **Available**, **Unavailable**, and **Wrap-up** possible states.
5. Select the desired agent state.

## Call Doesn't Record

**Problem**

When a user tries to record a call, the recording doesn't take place.

**Cause**

This is often due to configuration issues.

**Solution**

1. Set the phone to always record a call.
2. Make a call.

If the recording doesn't start, there are configuration problems. Check the configuration of the BroadWorks and third-party recorder.

If the recording does start:

1. Set the phone to record on demand.
2. Set up Wireshark to capture a trace of the network traffic between the phone and Broadworks when the problem occurs. When you have the trace, contact TAC for further assistance.

## An Emergency Call Doesn't Connect to Emergency Services

### Problem

A user tries to place an emergency call, but the call doesn't connect to the emergency services (fire, police, or emergency services operator).

### Solution

Check the emergency call configuration:

- Company Identifier or location request URL setup is incorrect. See [Configure a Phone to Make Emergency Calls, on page 267](#).
- An incorrect or blank emergency number exists in the Dial Plan setup. See [Edit the Dial Plan on the IP Phone, on page 404](#).

The location request servers (emergency call service provider) did not respond with a phone location, after multiple attempts.

## Presence Status Doesn't Work

### Problem

The phone doesn't show presence information.

### Solution

Use UC Communicator as a reference to verify that the account works.

## Phone Presence Message: Disconnected from Server

### Problem

Instead of presence information, the user sees the message `Disconnected from server`.

### Solution

- Check the Broadsoft server configuration to determine if IM&P service is enabled and assigned to that user.
- Check the phone configuration to determine if the phone can connect to the internet and get the XMPP messages.
- Check the XMPP Incoming and Outgoing messages printed in the syslog to make sure it can login successfully.

## Phone Cannot Access BroadSoft Directory for XSI

### Problem

The phone displays XSI directory access error.

### Solution

1. Check Broadsoft server configuration for the user login and SIP credentials.
2. Check error messages in syslog.
3. Check information on the error on the phone screen.
4. If HTTPS connection fails, check the error message on the phone screen and in the syslog.
5. Install custom CA for HTTPS connection if the BroadSoft certificate is not signed from phone built-in root CA.

## Phone Doesn't Show Contacts

### Problem

The phone doesn't display any contacts in the **All directories** screen when **Search All Enable** and **Browse Mode Enable** are set to **Yes**.

### Solution

1. Check that the personal address book is enabled in the phone.
2. Check that there are contacts in the local personal address book and the Bluetooth-paired phone.

## Phone Failed to Upload the PRT Logs to the Remote Server

### Problem

When you tried to generate the Problem Report Tool (PRT) logs on the phone, the generation of the PRT logs succeeded. However, the phone failed to upload the PRT logs to the remote server. The phone screen showed the `Error: 109 OR Report Problem` together with an unavailable URL of a compressed file (for example, tar.gz).

### Solution

Ensure that the web server is enabled on the phone, see [Configure the Network from the Phone, on page 329](#).

The `Error: 109` indicates that the PRT upload rule is incorrect.

The `Report problem` indicates that the PRT upload rule is empty.

To resolve the issue, you must enter a correct PRT upload rule on the phone administration web page.

# Saved Passwords Become Invalid after Downgrade

## Problem

You update certain passwords on a phone that uses Firmware Release 11.3(6) or later, and then downgrade the phone to Firmware Release 11.3(5) or older. In this scenario, the updated or saved passwords become invalid after the downgrade.

On the phone with Firmware Release 11.3(6) or later, even though you change the password back to the original one, this issue still occurs after the downgrade.

## Solution

For the Firmware Release 11.3(6) or later, if you update the passwords, you must reconfigure the passwords to avoid the downgrade issue. If not, this issue doesn't occur after the downgrade.

The following table shows the passwords that are affected by the downgrade issue:

**Table 68: Password List**

Category	Password Type
System Configuration	User Password
	Admin Password
Wi-Fi Profile (1-4)	Wi-Fi Password
	WEP Key
	PSK Passphrase
XSI Phone Service	Login Password
	SIP Password
Broadsoft XMPP	Password
XML Service	XML Password
LDAP	Password
Call Feature Settings	Auth Page Password
Subscriber Information	Password
XSI Line Service	Login Password
TR-069	ACS Password
	Connection Request Password
	BACKUP ACS Password

## Failed to Onboard the Phone to Webex

### Problem

A phone onboards with the EDOS device activation that uses phone MAC address, and it onboards to the Webex cloud. An administrator deletes the phone user from an organization in Webex Control Hub and then assigns the phone to another user. In this scenario, the phone fails to onboard to the Webex cloud even though it can connect to Webex Calling service. Specifically, the status of the phone in Control Hub is shown as "Offline".

### Solution

Manually perform a factory reset on the phone after a user is deleted in Control Hub. For more information about how to perform a factory reset, see one of the following topics for details:

- [Factory Reset the Phone with the Keypad, on page 446](#)
- [Perform Factory Reset from Phone Menu, on page 447](#)
- [Factory Reset the Phone from Phone Web Page, on page 447](#)

## Phone Display Problems

Your users may see unusual screen displays. Use the following sections to troubleshoot the problem.

### Phone Displays Irregular Fonts

#### Problem

The phone screen has smaller fonts than expected or there are unusual characters displayed. Examples of unusual characters are letters from a different alphabet from the characters that the locale uses.

#### Cause

Possible causes are:

- TFTP server does not have the correct set of locale and font files
- XML files or other files are specified as a font file
- The font and locale files did not download successfully.

#### Solution

- Font files and locale files must be in the same directory.
- Do not add or change files in the locale and font folder structure.
- On the phone web page, select **Admin Login** > **Advanced** > **Info** > **Status** and scroll to the **Locale Download Package** section to verify that the locale and font files downloaded successfully. If they did not, try the download again.



## Phone Screen Displays Boxes Instead of Asian Characters

### Problem

The phone is set for an Asian language, but the phone shows square boxes instead of Asian characters.

### Cause

Possible causes are:

- TFTP server does not have the correct set of locale and font files.
- The font and locale files did not download successfully.

### Solution

- Font files and locale files must be in the same directory.
- On the phone web page, select **Admin Login > Advanced > Info > Status** and scroll to the **Locale Download Package** section to verify that the locale and font files downloaded successfully. If they did not, try the download again.

## Report All Phone Issues from Phone Web Page

If you are working with Cisco TAC to troubleshoot a problem, they typically require the logs from the Problem Reporting Tool to help resolve the issue. You can generate PRT logs using the phone web page and upload them to a remote log server.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

---

- Step 1** Select **Info > Debug Info**.
- Step 2** In the **Problem Reports** section, click **Generate PRT**.
- Step 3** Enter the following information in the **Report Problem** screen:
- Enter the date that you experienced the problem in the **Date** field. The current date appears in this field by default.
  - Enter the time that you experienced the problem in the **Time** field. The current time appears in this field by default.
  - In the **Select Problem** drop-down list box, choose the description of the problem from the available options.
- Step 4** Click **Submit** in the **Report Problem** screen.
- The Submit button is enabled only if you select a value in the **Select Problem** drop-down list box.

You get a notification alert on the Phone Web page that indicates if the PRT upload was successful or not.

---

## Report Phone Issues from Webex Control Hub

You can issue a phone problem report remotely from the Webex Control Hub, after the phone successfully onboards to Webex cloud.

### Before you begin

- Access the customer view in <https://admin.webex.com/>.
- Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).
- Problem Report Tool is configured successfully. URL specified in the **PRT Upload Rule** field is valid. See, [Configure Problem Report Tool, on page 174](#).

### Procedure

---

**Step 1** From the Webex Control Hub, generate the problem report of a phone.

For more information, see [Webex for Cisco BroadWorks Solution Guide](#).

**Step 2** (Optional) Check the PRT generation status in any of the following ways:

- Access the phone administration web page, select **Info > Status > PRT Status**. The **PRT Generation Status** shows that the *Control Hub triggered PRT generation* is successful and the **PRT Upload Status** shows that the upload is successful.
  - On the phone, select **Applications > Status > Last problem report info**. The screen displays the report status is uploaded. The report generation time, the report upload time, and the PRT file name have the same value as shown in the phone administration web page.  
  
When you do not generate a PRT or you factory reset the phone, then **Last problem report info** doesn't appear.
  - Access the Webex Control Hub Help Desk and check the values of PRT generation. The values are identical with the values shown on the phone and on the phone administration web page.
- 

## Factory Reset the Phone from Phone Web Page

You can factory reset the phone from the phone web page. The reset only happens if the phone is idle. If the phone is not idle, the phone web page shows a message that the phone is busy and that you need to try again.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

---

- Step 1** Select **Info > Debug Info**.
- Step 2** In the **Factory Reset** section, click **Factory Reset**.
- Step 3** Click **Confirm factory reset**.
- 

## Reboot the Phone from the Webex Control Hub

You can reboot the phone from the Webex Control Hub remotely, after the phone successfully onboarded to Webex cloud. You can only reboot a phone that is in idle state. If it's in use, such as in a call, the phone doesn't reboot.

### Before you begin

- Access the customer view in <https://admin.webex.com/>.
- Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

---

- Step 1** From the Webex Control Hub, reboot a phone.
- For more information, see [Webex for Cisco BroadWorks Solution Guide](#).
- Step 2** (Optional) You can check the reboot reason from any of the following ways after the phone reboots successfully:
- Access the phone administration web page, select **Info > Status > Reboot History**. The reboot reason shows as cloud triggered.
  - On the phone, select **Applications > Status > Reboot history**. The **Reboot history** screen shows that the reboot is cloud triggered.
- 

## Report a Phone Problem Remotely

You can initiate a phone problem report remotely. The phone generates a problem report using the Cisco Problem Report Tool (PRT), with the problem description "Remote PRT Trigger". If you have configured an upload rule for problem reports, the phone uploads the problem report according to the upload rule.

You can see the status of the problem report generation and upload on the phone administration web page. When a problem report is successfully generated, you can download the problem report from the phone administration web page.

### Procedure

To initiate a phone problem report remotely, initiate a `SIP-NOTIFY` message from the server to the phone, with the Event specified as `prt-gen`.

## Capture Packets

For troubleshooting purposes you may need to gather a packet capture from an IP Phone.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

- Step 1** Select **Info > Debug Info**.
- Step 2** In the **Problem Report Tool** section, click the **Start Packet Capture** button in the **Packet Capture** field.
- Step 3** Choose **All** to capture all packets that the phone receives and select **Host IP Address** to capture packets only when source or destination is the IP address of the phone.
- Step 4** Make phone calls to and from the selected phone.
- Step 5** When you want to stop the packet capture, click **Stop Packet Capture**.
- Step 6** Click **Submit**.  
You see a file in the **Capture File** field. This file contains the filtered packets.

## Voice Quality Troubleshooting Tips

When you observe significant and persistent changes to metrics, use the following table for general troubleshooting information.

*Table 69: Changes to Voice Quality Metrics*

Metric Change	Condition
Conceal Ratio and Conceal Seconds increase significantly	Network impairment from packet loss or high jitter.

Metric Change	Condition
Conceal Ratio is near or at zero, but the voice quality is poor.	<ul style="list-style-type: none"> <li>• Noise or distortion in the audio channel such as echo or audio levels.</li> <li>• Tandem calls that undergo multiple encode/decode such as calls to a cellular network or calling card network.</li> <li>• Acoustic problems coming from a speakerphone, handsfree cellular phone or wireless headset.</li> </ul> Check packet transmit (TxCnt) and packet receive (RxCnt) counters to verify that voice packets are flowing.



**Note** Voice quality metrics do not account for noise or distortion, only frame loss.

## Phone Behavior During Times of Network Congestion

Anything that degrades network performance can affect Cisco IP Phone audio quality, and in some cases, can cause a call to drop. Sources of network degradation can include, but are not limited to, the following activities:

- Administrative tasks, such as an internal port scan or security scan
- Attacks that occur on your network, such as a Denial of Service attack

To reduce or eliminate any adverse effects to the phones, schedule administrative network tasks during a time when the phones are not being used or exclude the phones from testing.

## Where to Find Additional Information

If you have additional questions about troubleshooting your phone, see the *Cisco IP Phone 6800, 7800, and 8800 Series Multiplatform Phones Troubleshooting FAQ* in the the following Cisco website:

<https://www.cisco.com/c/en/us/support/collaboration-endpoints/ip-phone-8800-series-multiplatform-firmware/products-tech-notes-list.html>





## CHAPTER 18

# Monitoring Phone Systems

---

- [Monitoring Phone Systems Overview, on page 437](#)
- [Cisco IP Phone Status, on page 437](#)
- [Reboot Reasons, on page 443](#)

## Monitoring Phone Systems Overview

You can view a variety of information about the phone using the phone status menu on the phone and the phone web pages. This information includes:

- Device information
- Network setup information
- Network statistics
- Device logs
- Streaming statistics

This chapter describes the information that you can obtain from the phone web page. You can use this information to remotely monitor the operation of a phone and to assist with troubleshooting.

## Cisco IP Phone Status

The following sections describes how to view model information, status messages, and network statistics on the Cisco IP Phone.

- **Model Information:** Displays hardware and software information about the phone.
- **Status menu:** Provides access to screens that display the status messages, network statistics, and statistics for the current call.

You can use the information that displays on these screens to monitor the operation of a phone and to assist with troubleshooting.

You can also obtain much of this information, and obtain other related information, remotely through the phone web page.

## Display the Phone Information Window

### Procedure

---

**Step 1** Press **Applications** .

**Step 2** Select **Status > Product information**.

If the user is connected to a secure or authenticated server, a corresponding icon (lock or certificate) displays in the Phone Information Screen to the right of the server option. If the user is not connected to a secure or authenticated server, no icon appears.

The **Product information** screen might show the following information:

- Product name
- Serial number
- MAC address
- Software version
- Configuration version

The information displays only when it has been configured in the configuration file (cfg.xml).

- Hardware version
- VID (version ID)
- Certificate
- Customization

**Step 3** To exit the Model Information screen, press .

---

## View Phone Information

### Procedure

---

To check the current status of the Cisco IP Phone, click the **Info** tab.

The Info tab shows information about all phone extensions, including phone statistics and the registration status.

---



## View the Phone Status

### Procedure

---

- Step 1** Press **Settings** .
- Step 2** Select **Status > Phone status > Phone status**.

You can view the following information:

- **Elapsed time**—Total time elapsed since the last reboot of the system
  - **Tx (Packets)**—Transmitted packets from the phone.
  - **Rx (Packets)**—Received packets from the phone.
- 

## View the Status Messages on the Phone

### Procedure

---

- Step 1** Press **Settings** .
- Step 2** Select **Status > Status messages**.

You can view a log of the various phone statuses since provisioning was last done.

**Note** Status messages reflect UTC time and are not affected by the timezone settings on the phone.

- Step 3** Press **Back**.
- 

## View Download Status

You can view the download status from the phone web page when your user has difficulties with phone registration.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

---

- Step 1** Select **Info > Download Status**.
- Step 2** View the firmware upgrade, provisioning, and custom CA status details as described in the **Firmware Upgrade Status, Provisioning Status, Custom CA Status, and Screen Status**.

- Step 3** View the Manufacture Installed Certificate (MIC) renewal status details in the **MIC Cert Refresh Status** section.
- 

## Determine the IP Address of the Phone

A DHCP server assigns the IP address, so the phone must be booted up and connected to the subnetwork.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 100](#).

### Procedure

---

- Step 1** Select **Info > Status**.
- Step 2** Scroll to **IPv4 Information**. Current IP displays the IP address.
- Step 3** Scroll to **IPv6 Information**. Current IP displays the IP address.
- 

## View the Network Status

### Procedure

---

- Step 1** Press **Settings**.
- Step 2** Select **Status > Network status**.

You can view the following information:

- **Network type**—Indicates the type of Local Area Network (LAN) connection that the phone uses.
- **Network status**—Indicates if the phone is connected to a network.
- **IPv4 status**—IP address of the phone. You can see information on IP address, Addressing type, IP status, Subnet mask, Default router, Domain Name Server (DNS) 1, DNS 2 of the phone.
- **IPv6 status**—IP address of the phone. You can see information on IP address, Addressing type, IP status, Subnet mask, Default router, Domain Name Server (DNS) 1, DNS 2 of the phone.
- **VLAN ID**—VLAN ID of the phone.
- **MAC address**—Unique Media Access Control (MAC) address of the phone.
- **Host name**—Displays the current host name assigned to the phone.
- **Domain**—Displays the network domain name of the phone. Default: cisco.com
- **Switch port link**—Status of the switch port.

- **Switch port config**—Indicates speed and duplex of the network port.

## Voice Quality Monitoring

To measure the voice quality of calls that are sent and received within the network, Cisco IP Phones use these statistical metrics that are based on concealment events. The DSP plays concealment frames to mask frame loss in the voice packet stream.

- **Concealment Ratio metrics**—Show the ratio of concealment frames over total speech frames. An interval conceal ratio is calculated every 3 seconds.
- **Concealed Second metrics**—Show the number of seconds in which the DSP plays concealment frames due to lost frames. A severely “concealed second” is a second in which the DSP plays more than five percent concealment frames.





**Note** Concealment ratio and concealment seconds are primary measurements based on frame loss. A Conceal Ratio of zero indicates that the IP network is delivering frames and packets on time with no loss.

You can access voice quality metrics from the Cisco IP Phone using the Call Statistics screen or remotely by using Streaming Statistics.

## Display Call Statistics Screen

You can access the **Call statistics** menu on the phone to display detailed information of the recent calls. For example, call type, caller name, caller number.

### Procedure

- Step 1** Press **Applications** .
- Step 2** Select **Status > Phone status > Call statistics**.
- Step 3** To exit the Status menu, press **Back** .

## Call Statistics Fields

The following table describes the items on the Call Statistics screen.

*Table 70: Call Statistics Items for the Cisco IP Phone*

Item	Description
Call type	An outbound or inbound call.

Item	Description
Peer name	The name of the person who made or answered the call.
Peer phone	The phone number of the person who made or answered the call.
Encode codec	The method used to compress the outgoing audio.
Decode codec	The method used to decompress the incoming audio.
Call time	The time a call was made or answered.
Call ID	An identifier of the caller.

## View the Customization State in the Configuration Utility

After the RC download from the EDOS server completes, you can view the customization state of a phone using the web interface.

Here are the descriptions of the remote customization states:

- Open—The phone has booted for the first time and is not configured.
- Aborted—Remote customization is aborted due to other Provisioning like DHCP options.
- Pending—The profile has been downloaded from the EDOS server.
- Custom-Pending—The phone has downloaded a redirect URL from the EDOS server.
- Acquired—In the profile downloaded from the EDOS server, there is a redirect URL for provision configuration. If the redirect URL download from the provisioning server is successful, this state is displayed.
- Unavailable—Remote customization has stopped because the EDOS server responded with an empty provisioning file and the HTTP response was 200 OK.

### Procedure

---

**Step 1** On the Phone Web page, select **Admin Login > Info > Status**.

**Step 2** In the **Product Information** section, you can view the customization state of the phone in the **Customization** field.

If any provisioning is failing, you can view the details in the **Provisioning Status** section on the same page.

---

# Reboot Reasons

The phone stores the most recent five reasons that the phone was refreshed or rebooted. When the phone is reset to factory defaults, this information is deleted.

The following table describes the reboot and refresh reasons for the Cisco IP Phone.

Reason	Description
Upgrade	The reboot was a result of an upgrade operation (regardless whether the upgrade completed or failed).
Provisioning	The reboot was the result of changes made to parameter values by using the IP phone screen or phone web user interface, or as a result of synchronization.
SIP Triggered	The reboot was triggered by a SIP request.
RC	The reboot was triggered as a result of remote customization.
User Triggered	The user manually triggered a cold reboot.
IP Changed	The reboot was triggered after the phone IP address changed.

You can view the reboot history as follows:

- From the phone web user interface
- From the IP phone screen
- From the phone Status Dump file (<http://phoneIP/status.xml> or <http://phoneIP/admin/status.xml>)

## Reboot History on the Phone Web User Interface

On the **Info > System Status** page, the **Reboot History** section displays the device reboot history, the five most recent reboot dates and times, and a reason for the reboot. Each field displays the reason for the reboot and a time stamp that indicates when the reboot took place.

For example:

```
Reboot Reason 1: [08/13/14 06:12:38] User Triggered
Reboot Reason 2: [08/10/14 10:30:10] Provisioning
Reboot Reason 3: [08/10/14 10:28:20] Upgrade
```

The reboot history displays in reverse chronological order; the reason for the most recent reboot displays in **Reboot Reason 1**.

## Reboot History on the Cisco IP Phone Screen

**Reboot History** is located under **Apps > Admin Settings > Status** menu. In the Reboot History window, the reboot entries displays in reverse chronological order, similar to the sequence that displays on the phone web user interface.

## Reboot History in the Status Dump File

The reboot history is stored in the Status Dump file ([http://<phone\\_IP\\_address>/admin/status.xml](http://<phone_IP_address>/admin/status.xml)).

In this file, tags **Reboot\_Reason\_1** to **Reboot\_Reason\_3** store the reboot history, as shown in this example:

```
<Reboot_History>
<Reboot_Reason_1>[08/10/14 14:03:43]Provisioning</Reboot_Reason_1>
<Reboot_Reason_2>[08/10/14 13:58:15]Provisioning</Reboot_Reason_2>
<Reboot_Reason_3>[08/10/14 12:08:58]Provisioning</Reboot_Reason_3>
<Reboot_Reason_4>
<Reboot_Reason_5>
</Reboot_History/>
```



# CHAPTER 19

## Maintenance

- [Basic Reset, on page 445](#)

### Basic Reset



Performing a basic reset of a Cisco IP Phone provides a way to recover when the phone experiences an error. The reset provides a way to reset or restore various configuration and security settings.



**Note** When you set up emergency calls, the phone requests an updated location whenever a person restarts the phone.

The following table describes the ways to perform a basic reset. You can reset a phone with any of these operations after the phone has started up. Choose the operation that is applicable for your situation.

**Table 71: Basic Reset Methods**

Operation	Action	Explanation
Restart phone	Press <b>Services, Applications</b>  , or <b>Directories</b> and then press <b>**#**</b> .	Resets any user and network setup changes that you have made, but that the phone has not written to its Flash memory, to previously saved settings, then restarts the phone.
Reset settings		Restores phone configuration or settings to factory default.
	To reset settings, press <b>Applications</b>  > <b>Admin Settings</b> > <b>Custom Reset</b> .	Restores phone configuration or settings to noncustomized default.



---

**Note** When you set up emergency calls, the phone requests an updated location whenever the you do the following actions:

- Registers the phone with the call server.
  - Restarts the phone (phone is registered).
  - Changes the network interface that is used for the SIP registration.
  - Changes the IP address of the phone.
- 

## Factory Reset the Phone with the Keypad

Use these steps to reset the phone to factory default settings using the phone keypad.

You have two methods to perform the factory reset by using the keypad:

- **Method 1** (recommended): Press # > **123456789\*0#**
- **Method 2**: Press **0 > 369#**

### Before you begin

You must know if your phone is an original hardware release or if the hardware has been updated and re-released.

### Procedure

---

**Step 1** Unplug the phone:

- If using PoE, unplug the LAN cable.
- If using the power cube, unplug the power cube.

**Step 2** Wait 5 seconds.

**Step 3** Do one of the following actions:

- **Method 1**: Press and hold # and plug the phone back in.
- **Method 2**: Press and hold 0 and plug the phone back in.

The phone begins the reboot process. The headset button and the speaker button light up.

**Step 4** On earlier hardware versions, the Mute button lights up. Wait for the Mute button to turn off.

**Step 5** Do one of the following actions:

- **Method 1**: Press **123456789\*0#** in sequence.

When you press **1**, the lights on the headset button turns off. The light on the Select button flashes when a button is pressed.

After you press these buttons, the phone goes through the factory reset process.

If you press the buttons out of sequence, the phone powers on normally.



**Caution** Do not power down the phone until it completes the factory reset process, and the main screen appears.

- **Method 2:** Press **369#** in sequence.

After you press these buttons, the phone still remains on the same screen, and all LEDs change to solid green.

- Step 6** If you use the **Method 2**, unplug and plug in the phone again to reboot it.  
After the phone reboots, the main screen appears.

---

## Perform Factory Reset from Phone Menu

### Procedure

---

- Step 1** Press **Settings**.
- Step 2** Select **Device administration > Factory reset**.
- Step 3** To restore phone configuration or settings to factory default, press **OK**.
- 

## Factory Reset the Phone from Phone Web Page

You can restore your phone to its original manufacturer settings from the phone web page. After you reset the phone, you can reconfigure it.

### Procedure

---

Reset your phone from the phone web page from one of the methods:

- Enter the URL in a supported web browser and click **Confirm Factory Reset**.

You can enter URL in the format:

```
http://<Phone IP>/admin/factory-reset
```

where:

Phone IP = actual IP address of your phone.

/admin = path to access admin page of your phone.

factory-reset = command that you need to enter in the phone web page to factory-reset your phone.

- On the phone web page, select **Admin Login > Advanced > Info > Debug Info**. Click **Factory Reset** in the **Factory Reset** section and confirm the factory reset message in the next screen. Click **Submit All Changes**.
-

## Identify Phone Issues with a URL in the Phone Web Page

When the phone doesn't work or doesn't register, a network error or any misconfiguration might be the cause. To identify the cause, add a specific IP address or a domain name to the phone admin page. Then, try to access so that the phone can ping the destination and display the cause.

### Procedure

---

In a supported web browser, enter a URL that consists of your phone IP address and the destination IP that you want to ping. Enter the URL using the format:

`http://<Phone IP>/admin/ping?<ping destination>`, where:

*<Phone IP>* = actual IP address of your phone.

*/admin* = path to the access admin page of your phone.

*<ping destination>* = any IP address or domain name that you want to ping.

The ping destination allows only alphanumeric characters, '-', and '\_' (underscores). Otherwise the phone shows an error on the web page. If the *<ping destination>* includes spaces, the phone uses only the first part of the address as the pinging destination.

For example, to ping the 192.168.1.1 address:

`http://<Phone IP>/admin/ping?192.168.1.1`

---



# APPENDIX **A**

## Technical Details

- [Network Protocols](#), on page 449
- [Phone Behavior During Times of Network Congestion](#), on page 453
- [SIP and NAT Configuration](#), on page 453
- [Cisco Discovery Protocol](#), on page 458
- [LLDP-MED](#), on page 459
- [Final Network Policy Resolution and QoS](#), on page 464

## Network Protocols

The Cisco IP Conference Phone 8832 supports several industry-standard and Cisco network protocols that are required for voice communication. The following table provides an overview of the network protocols that the phones support.

**Table 72: Supported Network Protocols on the Cisco IP Conference Phone**

Network Protocol	Purpose	Usage Notes
Bootstrap Protocol (BootP)	BootP enables a network device, such as the phone, to discover certain startup information, such as its IP address.	—
Cisco Discovery Protocol (CDP)	CDP is a device-discovery protocol that runs on all Cisco-manufactured equipment.  A device can use CDP to advertise its existence to other devices and receive information about other devices in the network.	The phone uses CDP to communicate information such as auxiliary VLAN ID, per port power management details, and Quality of Service (QoS) configuration information with the Cisco Catalyst switch.

Network Protocol	Purpose	Usage Notes
Dynamic Host Configuration Protocol (DHCP)	<p>DHCP dynamically allocates and assigns an IP address to network devices.</p> <p>DHCP enables you to connect an IP phone into the network and have the phone become operational without the need to manually assign an IP address or to configure additional network parameters.</p>	<p>DHCP is enabled by default. If disabled, you must manually configure the IP address, subnet mask, gateway, and a TFTP server on each phone locally.</p> <p>We recommend that you use DHCP custom option 150. With this method, you configure the TFTP server IP address as the option value. For additional supported DHCP configurations, see the documentation for your particular Cisco Unified Communications Manager release.</p> <p><b>Note</b> If you cannot use option 150, use DHCP option 66.</p>
Hypertext Transfer Protocol (HTTP)	HTTP is the standard protocol for transfer of information and movement of documents across the Internet and the web.	Phones use HTTP for XML services, provisioning, upgrade and for troubleshooting purposes.
Hypertext Transfer Protocol Secure (HTTPS)	Hypertext Transfer Protocol Secure (HTTPS) is a combination of the Hypertext Transfer Protocol with the SSL/TLS protocol to provide encryption and secure identification of servers.	<p>Web applications with both HTTP and HTTPS support have two URLs configured. phones that support HTTPS choose the HTTPS URL.</p> <p>A lock icon is displayed to the user if the connection to the service is via HTTPS.</p>
IEEE 802.1X	<p>The IEEE 802.1X standard defines a client-server-based access control and authentication protocol that restricts unauthorized clients from connection to a LAN through publicly accessible ports.</p> <p>Until the client is authenticated, 802.1X access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.</p>	<p>The phone implements the IEEE 802.1X standard through support for the following authentication methods: EAP-FAST and EAP-TLS.</p> <p>When 802.1X authentication is enabled on the phone, you should disable the voice VLAN.</p>



Network Protocol	Purpose	Usage Notes
Session Description Protocol (SDP)	SDP is the portion of the SIP protocol that determines which parameters are available during a connection between two endpoints. Conferences are established by using only the SDP capabilities that all endpoints in the conference support.	SDP capabilities, such as codec types, DTMF detection, and comfort noise, are normally configured on a global basis by Cisco Unified Communications Manager or Media Gateway in operation. Some SIP endpoints may allow configuration of these parameters on the endpoint itself.
Session Initiation Protocol (SIP)	SIP is the Internet Engineering Task Force (IETF) standard for multimedia conferencing over IP. SIP is an ASCII-based application-layer control protocol (defined in RFC 3261) that can be used to establish, maintain, and terminate calls between two or more endpoints.	Like other VoIP protocols, SIP is designed to address the functions of signaling and session management within a packet telephony network. Signaling allows call information to be carried across network boundaries. Session management provides the ability to control the attributes of an end-to-end call.
Secure Real-Time Transfer protocol (SRTP)	SRTP is an extension of the Real-Time Protocol (RTP) Audio/Video Profile and ensures the integrity of RTP and Real-Time Control Protocol (RTCP) packets providing authentication, integrity, and encryption of media packets between two endpoints.	Phones use SRTP for media encryption.
Transmission Control Protocol (TCP)	TCP is a connection-oriented transport protocol.	Phones use TCP to connect to Cisco Unified Communications Manager and to access XML services.
Transport Layer Security (TLS)	TLS is a standard protocol for securing and authenticating communications.	When security is implemented, phones use the TLS protocol when securely registering with the Cisco Unified Communications Manager. For more information, see the documentation for your particular Cisco Unified Communications Manager release.
Trivial File Transfer Protocol (TFTP)	TFTP allows you to transfer files over the network.  On the phone, TFTP enables you to obtain a configuration file specific to the phone type.	TFTP requires a TFTP server in your network, which can be automatically identified from the DHCP server. If you want a phone to use a TFTP server other than the one specified by the DHCP server, you must manually assign the IP address of the TFTP server by using the Network Setup menu on the phone.  For more information, see the documentation for your particular Cisco Unified Communications Manager release.
User Datagram Protocol (UDP)	UDP is a connectionless messaging protocol for delivery of data packets.	UDP is used only for RTP streams. SIP signaling on the phones do not support UDP.

# Phone Behavior During Times of Network Congestion

Anything that degrades network performance can affect phone audio and, in some cases, can cause a call to drop. Sources of network degradation can include, but are not limited to, the following activities:

- Administrative tasks, such as an internal port scan or security scan.
- Attacks that occur on your network, such as a Denial of Service attack.

## SIP and NAT Configuration

### SIP and the Cisco IP Phone

The Cisco IP Phone uses Session Initiation Protocol (SIP), which allows interoperability with all IT service providers that support SIP. SIP is an IETF-defined signaling protocol that controls voice communication sessions in an IP network.

SIP handles signaling and session management within a packet telephony network. *Signaling* allows call information to be carried across network boundaries. *Session management* controls the attributes of an end-to-end call.

In typical commercial IP telephony deployments, all calls go through a SIP Proxy Server. The receiving phone is called the SIP user agent server (UAS), while the requesting phone is called the user agent client (UAC).

SIP message routing is dynamic. If a SIP proxy receives a request from a UAS for a connection but cannot locate the UAC, the proxy forwards the message to another SIP proxy in the network. When the UAC is located, the response routes back to the UAS, and the two UAs connect using a direct peer-to-peer session. Voice traffic transmits between UAs over dynamically assigned ports using Real-time Protocol (RTP).

RTP transmits real-time data such as audio and video; RTP does not guarantee real-time delivery of data. RTP provides mechanisms for the sending and receiving applications to support streaming data. Typically, RTP runs on top of UDP.

### SIP Over TCP

To guarantee state-oriented communications, the Cisco IP Phone can use TCP as the transport protocol for SIP. This protocol provides *guaranteed delivery* that assures that lost packets are retransmitted. TCP also guarantees that the SIP packages are received in the same order that they were sent.

TCP overcomes the problem of UDP port-blocking by corporate firewalls. With TCP, new ports do not need to be open or packets dropped, because TCP is already in use for basic activities, such as internet browsing or e-commerce.

### SIP Proxy Redundancy

An average SIP Proxy Server can handle tens of thousands of subscribers. A backup server allows an active server to be temporarily switched out for maintenance. The phone supports the use of backup servers to minimize or eliminate service disruption.

A simple way to support proxy redundancy is to specify a SIP Proxy Server in the phone configuration profile. The phone sends a DNS NAPTR or SRV query to the DNS server. If configured, the DNS server returns SRV

records that contain a list of servers for the domain, with their hostnames, priority, listening ports, and so forth. The phone tries to contact the servers in the order of the priority. The server with a lower number has a higher priority. Up to six NAPTR records and twelve SRV records are supported in a query.

When the phone fails to communicate with the primary server, the phone can failover to a lower-priority server. If configured, the phone can restore the connection back to the primary. Failover and failback support switches between servers with different SIP transport protocols. The phone doesn't perform failback to the primary server during an active call until the call ends and the failback conditions are met.

### Example of Resource Records from the DNS Server

```
aslbsoft      3600      IN NAPTR 50  50  "s"  "SIPS+D2T"  ""  _sips._tcp.tlstest
              3600      IN NAPTR 90  50  "s"  "SIP+D2T"   ""  _sip._tcp.tcptest
              3600      IN NAPTR 100 50  "s"  "SIP+D2U"   ""  _sip._udp.udptest

_sips._tcp.tlstest SRV 1 10 5061 srv1.sipurash.com.
                  SRV 2 10 5060 srv2.sipurash.com.
_sip._tcp.tcptest  SRV 1 10 5061 srv3.sipurash.com.
                  SRV 2 10 5060 srv4.sipurash.com.
_sip._udp.udptest  SRV 1 10 5061 srv5.sipurash.com.
                  SRV 2 10 5060 srv6.sipurash.com.

srv1      3600      IN      A      1.1.1.1
srv2      3600      IN      A      2.2.2.2
srv3      3600      IN      A      3.3.3.3
srv4      3600      IN      A      4.4.4.4
srv5      3600      IN      A      5.5.5.5
srv6      3600      IN      A      6.6.6.6
```

The following example shows the priority of the servers from the perspective of the phone.

Priority	IP Address	SIP Protocol	Status
1st	1.1.1.1	TLS	UP
2nd	2.2.2.2	TLS	UP
3rd	3.3.3.3	TCP	UP
4th	4.4.4.4	TCP	UP
5th	5.5.5.5	UDP	UP
6th	6.6.6.6	UDP	UP

The phone always sends SIP messages to the available address with the top priority and with the status UP in the list. In the example, the phone sends all the SIP messages to the address 1.1.1.1. If the address 1.1.1.1 in the list is marked with the status DOWN, the phone communicates with 2.2.2.2 instead. The phone can restore the connection back to 1.1.1.1 when the specified failback conditions are met. For more details about failover and failback, see [SIP Proxy Failover, on page 454](#) and [SIP Proxy Failback, on page 455](#).

## SIP Proxy Failover

The phone performs a failover in any of these cases:

- The phone sends SIP messages and doesn't get responses from the server.
- The server responds with a code that matches the specified code in **Try Backup RSC**.
- The phone gets a TCP disconnection request.

We strongly recommend that you set the **Auto Register When Failover** to **Yes** when **SIP Transport** is set to **Auto**.

You can also configure this extension-specific parameters in the configuration file:



```
<SIP_Transport_n_ua="na">Auto</SIP_Transport_n_>
<Auto_Register_When_Failover_n_ua="na">Yes</Auto_Register_When_Failover_n_>
```

where *n* is the extension number.

### Phone Failover Behavior

When the phone fails to communicate with the currently connected server, it refreshes the server list status. The unavailable server is marked with the status DOWN in the server list. The phone tries to connect to the top-priority server with the status UP in the list.

In the following example, the addresses 1.1.1.1 and 2.2.2.2 aren't available. The phone sends SIP messages to 3.3.3.3, which has the top priority among the servers with the status UP.

Priority	IP Address	SIP Protocol	Status
1st	1.1.1.1	TLS	DOWN
2nd	2.2.2.2	TLS	DOWN
3rd	3.3.3.3	TCP	UP
4th	4.4.4.4	TCP	UP
5th	5.5.5.5	UDP	UP
6th	6.6.6.6	UDP	UP

In the following example, there are two SRV records from the DNS NAPTR response. For each SRV record, there are three A records (IP addresses).

Priority	IP Address	SIP Protocol	Server	Status
1st	1.1.1.1	UDP	SRV1	DOWN
2nd	1.1.1.2	UDP	SRV1	UP
3rd	1.1.1.3	UDP	SRV1	UP
4th	2.2.2.1	TLS	SRV2	UP
5th	2.2.2.2	TLS	SRV2	UP
6th	2.2.2.3	TLS	SRV2	UP

Let's assume that the phone failed to connect to 1.1.1.1 and then registered to 1.1.1.2. When 1.1.1.2 goes down, phone behavior depends on the setting of **Proxy Fallback Intvl**.

- When **Proxy Fallback Intvl** is set to **0**, the phone tries with the addresses in this order: 1.1.1.1, 1.1.1.3, 2.2.2.1, 2.2.2.2, 2.2.2.3.
- When **Proxy Fallback Intvl** is set to a value other than zero, the phone tries with the addresses in this order: 1.1.1.3, 2.2.2.1, 2.2.2.2, 2.2.2.3.

## SIP Proxy Fallback

The proxy fallback requires a value other than zero specified in the **Proxy Fallback Intvl** field on the **Ext (n)** tab in the phone web interface. If you set this field to 0, the SIP proxy fallback feature is disabled. You can also configure this extension-specific parameter in the configuration file in this format:

```
<Proxy_Fallback_Intvl_n_ua="na">60</Proxy_Fallback_Intvl_n_>
```

where *n* is the extension number.

The time when the phone triggers a fallback depends on the phone configuration and the SIP transport protocols in use.

To enable the phone to perform failback between different SIP transport protocols, set **SIP Transport** to **Auto** on the **Ext (n)** tab in the phone web interface. You can also configure this extension-specific parameter in the configuration file with the following XML string:

```
<SIP_Transport_n_ ua="na">Auto</SIP_Transport_n_>
```

where *n* is the extension number.

### Failback from a UDP Connection

The failback from a UDP connection is triggered by SIP messages. In the following example, the phone first failed to register to 1.1.1.1 (TLS) at the time T1 since there's no response from the server. When SIP Timer F expires, the phone registers to 2.2.2.2 (UDP) at the time T2 (T2=T1+SIP Timer F). The current connection is on 2.2.2.2 via UDP.

Priority	IP Address	SIP Protocol	Status	
1st	1.1.1.1	TLS	DOWN	T1 (Down time)
2nd	2.2.2.2	UDP	UP	
3rd	3.3.3.3	TCP	UP	

The phone has the following configuration:

```
<Proxy_Fallback_Intvl_n_ ua="na">60</Proxy_Fallback_Intvl_n_>
<Register_Expires_n_ ua="na">3600</Register_Expires_n_>
<SIP_Timer_F ua="na">16</SIP_Timer_F>
```

where *n* is the extension number.

The phone refreshes the registration at time T2 (T2=(3600-16)\*78%). The phone checks the address list for the availability of the IP addresses and the down time. If T2-T1 >= 60, the failed server 1.1.1.1 resumes back to UP and the list is updated to the following. The phone sends SIP messages to 1.1.1.1.

Priority	IP Address	SIP Protocol	Status
1st	1.1.1.1	TLS	UP
2nd	2.2.2.2	UDP	UP
3rd	3.3.3.3	TCP	UP

### Failback from a TCP or TLS Connection

The failback from a TCP or TLS connection is triggered by the parameter **Proxy Fallback Intvl**. In the following example, the phone failed to register to 1.1.1.1 (UDP) at the time T1 and thus registered to 2.2.2.2 (TCP). The current connection is on 2.2.2.2 via TCP.

Priority	IP Address	SIP Protocol	Status	
1st	1.1.1.1	UDP	DOWN	T1 (Down time)
2nd	2.2.2.2	TCP	UP	
3rd	3.3.3.3	TLS	UP	

The phone has the following configuration:

```
<Proxy_Fallback_Intvl_n_ ua="na">60</Proxy_Fallback_Intvl_n_>
<Register_Expires_n_ ua="na">3600</Register_Expires_n_>
<SIP_Timer_F ua="na">16</SIP_Timer_F>
```

where *n* is the extension number.

The proxy fallback interval (60 seconds) counts down from T1. The phone triggers proxy failback at the time of T1+60. If you set the proxy fallback interval to 0 in this example, the phone keeps the connection on 2.2.2.2.

## Dual Registration

The phone always registers to both primary (or primary outbound) and alternate (or alternate outbound) proxies. After registration, the phone sends out Invite and Non-Invite SIP messages through primary proxy first. If there is no response for the new INVITE from the primary proxy, after timeout, the phone attempts to connect with the alternate proxy. If the phone fails to register to the primary proxy, it sends an INVITE to the alternate proxy without trying the primary proxy.

Dual registration is supported on a per-line basis. Three added parameters can be configured through web user interface and remote provisioning:

- Alternate Proxy—Default is empty.
- Alternate Outbound Proxy—Default is empty.
- Dual Registration—Default is NO (turned off).

After you configure the parameters, reboot the phone for the feature to take effect.



---

**Note** Specify a value for primary proxy (or primary outbound proxy) and alternate proxy (or alternate outbound proxy) for the feature to function properly.

---

### Dual Registration and DNS SRV Limitations

- When Dual Registration is enabled, DNS SRV Proxy Fallback or Recovery must be disabled.
- Do not use Dual Registration along with other Fallback or Recovery mechanisms. For example: Broadsoft mechanism.
- There is no recovery mechanism for feature request. However, the administrator can adjust the reregistration time for a prompt update of the registration state for primary and alternate proxy.

### Dual Registration and Alternate Proxy

When the Dual Register parameter is set to **No**, Alternate Proxy is ignored.

## RFC3311

The Cisco IP Phone supports RFC-3311, the SIP UPDATE Method.

## SIP NOTIFY XML-Service

The Cisco IP Phone supports the SIP NOTIFY XML-Service event. On receipt of a SIP NOTIFY message with an XML-Service event, the phone challenges the NOTIFY with a 401 response if the message does not contain correct credentials. The client must furnish the correct credentials using MD5 digest with the SIP account password for the corresponding line of the IP phone.

The body of the message can contain the XML event Message. For example:

```
<CiscoIPPhoneExecute>  
<ExecuteItem Priority="0" URL="http://xmlserver.com/event.xml"/>  
</CiscoIPPhoneExecute>
```

Authentication:

```
challenge = MD5( MD5(A1) ":" nonce ":" nc-value ":" cnonce ":" qop-value
":" MD5(A2) )
where A1 = username ":" realm ":" passwd
and A2 = Method ":" digest-uri
```

## NAT Transversal with Phones

Network Address Translation (NAT) allows multiple devices to share a single, public, routable, IP address to establish connections over the Internet. NAT is present in many broadband access devices to translate public and private IP addresses. For VoIP to coexist with NAT, NAT traversal is required.

Not all service providers provide NAT traversal. If your service provider does not provide NAT traversal, you have several options:

- **NAT Mapping with Session Border Controller:** We recommend that you choose an service provider that supports NAT mapping through a Session Border Controller. With NAT mapping provided by the service provider, you have more choices in selecting a router.
- **NAT Mapping with SIP-ALG Router:** NAT mapping can be achieved by using a router that has a SIP Application Layer Gateway (ALG). By using a SIP-ALG router, you have more choices in selecting an service provider.
- **NAT Mapping with a Static IP Address:** NAT mapping with an external (public) static IP address can be achieved to ensure interoperability with the service provider. The NAT mechanism used in the router must be symmetric. For more information, see [Determine Symmetric or Asymmetric NAT, on page 396](#).

Use NAT mapping only if the service provider network does not provide a Session Border Controller functionality. For more information on how to configure NAT mapping with a static IP, see [Configure NAT Mapping with the Static IP Address , on page 391](#).

- **NAT Mapping with STUN:** If the service provider network does not provide a Session Border Controller functionality and if the other requirements are met, it is possible to use Session Traversal Utilities for NAT (STUN) to discover the NAT mapping. For information on how to configure NAT mapping with STUN, see [Configure NAT mapping with STUN, on page 395](#).

### NAT Mapping with Session Border Controller

We recommend that you choose an service provider that supports NAT mapping through a Session Border Controller. With NAT mapping provided by the service provider, you have more choices in selecting a router.

### NAT Mapping with SIP-ALG Router

NAT mapping can be achieved by using a router that has a SIP Application Layer Gateway (ALG). By using a SIP-ALG router, you have more choices in selecting an service provider.

## Cisco Discovery Protocol

Cisco Discovery Protocol (CDP) is negotiation-based and determines which virtual LAN (VLAN) the Cisco IP Phone resides in. If you are using a Cisco switch, Cisco Discovery Protocol (CDP) is available and is enabled by default. CDP has these attributes:

- Obtains the protocol addresses of neighboring devices and discovers the platform of those devices.

- Shows information about the interfaces your router uses.
- Is media and protocol-independent.

If you are using a VLAN without CDP, you must enter a VLAN ID for the Cisco IP Phone.

## LLDP-MED

The Cisco IP Phone supports Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) for deployment with Cisco or other Third-Party network connectivity devices that use a Layer 2 auto discovery mechanism. Implementation of LLDP-MED is done in accordance with IEEE 802.1AB (LLDP) Specification of May 2005, and ANSI TIA-1057 of April 2006.

The Cisco IP Phone operates as a LLDP-MED Media End Point Class III device with direct LLDP-MED links to Network Connectivity Devices, according to the Media Endpoint Discovery Reference Model and Definition (ANSI TIA-1057 Section 6).

The Cisco IP Phone supports only the following limited set of Type-Length-Values (TLV) as an LLDP-MED Media Endpoint device class III:

- Chassis ID TLV
- Port ID TLV
- Time to live TLV
- Port Description TLV
- System Name TLV
- System Capabilities TLV
- IEEE 802.3 MAC/PHY Configuration/Status TLV (for wired network only)
- LLDP-MED Capabilities TLV
- LLDP-MED Network Policy TLV (for application type=Voice only)
- LLDP-MED Extended Power-Via-MDI TLV (for wired network only)
- LLDP-MED Firmware Revision TLV
- End of LLDPDU TLV

The outgoing LLDPDU contains all the preceding TLVs if applicable. For the incoming LLDPDU, the LLDPDU is discarded if any of the following TLVs are missing. All other TLVs are not validated and ignored.

- Chassis ID TLV
- Port ID TLV
- Time to live TLV
- LLDP-MED Capabilities TLV
- LLDP-MED Network Policy TLV (for application type=Voice only)
- End of LLDPDU TLV

The Cisco IP Phone sends out the shutdown LLDPDU if applicable. The LLDPDU frame contains the following TLVs:

- Chassis ID TLV
- Port ID TLV
- Time to live TLV
- End of LLDPDU TLV

There are some restrictions in the implementation of LLDP-MED on the Cisco IP Phones:

- Storage and retrieval of neighbor information are not supported.
- SNMP and corresponding MIBs are not supported.
- Recording and retrieval of statistical counters are not supported.
- Full validation of all TLVs does not take place; TLVs that do not apply to the phones are ignored.
- Protocol state machines as stated in the standards are used only for reference.

## Chassis ID TLV

For the outgoing LLDPDU, the TLV supports subtype=5 (Network Address). When the IP address is known, the value of the Chassis ID is an octet of the INAN address family number followed by the octet string for the IPv4 address used for voice communication. If the IP address is unknown, the value for the Chassis ID is 0.0.0.0. The only INAN address family supported is IPv4. Currently, the IPv6 address for the Chassis ID is not supported.

For the incoming LLDPDU, the Chassis ID is treated as an opaque value to form the MSAP identifier. The value is not validated against its subtype.

The Chassis ID TLV is mandatory as the first TLV. Only one Chassis ID TLV is allowed for the outgoing and incoming LLDPDUs.

## Port ID TLV

For the outgoing LLDPDU, the TLV supports subtype=3 (MAC address). The 6 octet MAC address for the Ethernet port is used for the value of Port ID.

For the incoming LLDPDU, the Port ID TLV is treated as an opaque value to form the MSAP identifier. The value is not validated against its subtype.

The Port ID TLV is mandatory as the second TLV. Only one Port ID TLV is allowed for the outgoing and incoming LLDPDUs.

## Time to Live TLV

For the outgoing LLDPDU, the Time to Live TTL value is 180 seconds. This differs from the 120-second value that the standard recommends. For the shutdown LLDPDU, the TTL value is always 0.

The Time to Live TLV is mandatory as the third TLV. Only one Time to Live TLV is allowed for the outgoing and incoming LLDPDUs.

## End of LLDPDU TLV

The value is 2-octet, all zero. This TLV is mandatory and only one is allowed for the outgoing and incoming LLDPDUs.

## Port Description TLV

For the outgoing LLDPDU, in the Port Description TLV, the value for the port description is the same as “Port ID TLV” for CDP. The incoming LLDPDU, the Port Description TLV, is ignored and not validated. Only one Port Description TLV is allowed for outgoing and incoming LLDPDUs.

## System Name TLV

For the Cisco IP Phone, the value is SEP+MAC address.

**Example:** SEPAC44F211B1D0

The incoming LLDPDU, the System Name TLV, is ignored and not validated. Only one System Name TLV is allowed for the outgoing and incoming LLDPDUs.

## System Capabilities TLV

For the outgoing LLDPDU, in the System Capabilities TLV, the bit values for the 2 octet system capabilities fields should be set for Bit 2 (Bridge) and Bit 5 (Phone) for a phone with a PC port. If the phone does not have a PC port, only Bit 5 should be set. The same system capability value should be set for the enabled capability field.

For the incoming LLDPDU, the System Capabilities TLV is ignored. The TLV is not validated semantically against the MED device type.

The System Capabilities TLV is mandatory for outgoing LLDPDUs. Only one System Capabilities TLV is allowed.

## Management Address TLV

The TLV identifies an address associated with the local LLDP agent (that may be used to reach higher layer entities) to assist discovery by network management. The TLV allows the inclusion of both the system interface number and an object identifier (OID) that are associated with this management address, if either or both are known.

- TLV information string length—This field contains the length (in octets) of all the fields in the TLV information string.
- Management address string length—This field contains the length (in octets) of the management address subtype + management address fields.

## System Description TLV

The TLV allows the network management to advertise the system description.

- TLV information string length—This field indicates the exact length (in octets) of the system description.

- System description—This field contains an alphanumeric string that is the textual description of the network entity. The system description includes the full name and version identification of the system hardware type, software operating system, and networking software. If implementations support IETF RFC 3418, the sysDescr object should be used for this field.

## IEEE 802.3 MAC/PHY Configuration/Status TLV

The TLV is not for autonegotiation, but for troubleshooting purposes. For the incoming LLDPDU, the TLV is ignored and not validated. For the outgoing LLDPDU, for the TLV, the octet value autonegotiation support/status should be:

- Bit 0—Set to 1 to indicate that the autonegotiation support feature is supported.
- Bit 1—Set to 1 to indicate that autonegotiation status is enabled.
- Bit 2-7—Set to 0.

The bit values for the 2 octets PMD autonegotiation advertised capability field should be set to:

- Bit 13—10BASE-T half duplex mode
- Bit 14—10BASE-T full duplex mode
- Bit 11—100BASE-TX half duplex mode
- Bit 10—100BASE-TX full duplex mode
- Bit 15—Unknown

Bit 10, 11, 13 and 14 should be set.

The value for 2 octets operational MAU type should be set to reflect the real operational MAU type:

- 16—100BASE-TX full duplex
- 15—100BASE-TX half duplex
- 11—10BASE-T full duplex
- 10—10BASE-T half duplex

For example, usually, the phone is set to 100BASE-TX full duplex. The value 16 should then be set. The TLV is optional for a wired network and not applicable for a wireless network. The phone sends out this TLV only when in wired mode. When the phone is not set for autonegotiation but specific speed/duplexity, for the outgoing LLDPDU TLV, bit 1 for the octet value autonegotiation support/status should be clear (0) to indicate that autonegotiation is disabled. The 2 octets PMD autonegotiation advertised capability field should be set to 0x8000 to indicate unknown.

## LLDP-MED Capabilities TLV

For the outgoing LLDPDU, the TLV should have the device type 3 (End Point Class III) with the following bits set for 2-octet Capability field:



Bit Position	Capability
0	LLDP-MED Capabilities
1	Network Policy
4	Extended Power via MDI-PD
5	Inventory

For the incoming TLV, if the LLDP-MED TLV is not present, the LLDPDU is discarded. The LLDP-MED Capabilities TLV is mandatory and only one is allowed for the outgoing and incoming LLDPDUs. Any other LLDP-MED TLVs will be ignored if they present before the LLDP-MED Capabilities TLV.

## Network Policy TLV

In the TLV for the outgoing LLDPDU, before the VLAN or DSCP is determined, the Unknown Policy Flag (U) is set to 1. If the VLAN setting or DSCP is known, the value is set to 0. When the policy is unknown, all other values are set to 0. Before the VLAN is determined or used, the Tagged Flag (T) is set to 0. If the tagged VLAN (VLAN ID > 1) is used for the phone, the Tagged Flag (T) is set to 1. Reserved (X) is always set to 0. If the VLAN is used, the corresponding VLAN ID and L2 Priority will be set accordingly. VLAN ID valid value is range from 1-4094. However, VLAN ID=1 will never be used (limitation). If DSCP is used, the value range from 0-63 is set accordingly.

In the TLV for the incoming LLDPDU, Multiple Network Policy TLVs for different application types are allowed.

## LLDP-MED Extended Power-Via-MDI TLV

In the TLV for the outgoing LLDPDU, the binary value for Power Type is set to “0 1” to indicate the power type for phone is PD Device. The Power source for the phone is set to “PSE and local” with binary value “1 1”. The Power Priority is set to binary “0 0 0 0” to indicate unknown priority while the Power Value is set to maximum power value. The Power Value for the Cisco IP Phone is 12900mW.

For the incoming LLDPDU, the TLV is ignored and not validated. Only one TLV is allowed in the outgoing and incoming LLDPDUs. The phone will send out the TLV for the wired network only.

The LLDP-MED standard was originally drafted in the context of Ethernet. Discussion is ongoing for LLDP-MED for Wireless Networks. Refer to ANSI-TIA 1057, Annex C, C.3 Applicable TLV for VoWLAN, table 24. It is recommended that the TLV is not applicable in the context of the wireless network. This TLV is targeted for use in the context of PoE and Ethernet. The TLV, if added, will not provide any value for network management or power policy adjustment at the switch.

## LLDP-MED Inventory Management TLV

This TLV is optional for Device Class III. For the outgoing LLDPDU, we support only Firmware Revision TLV. The value for the Firmware Revision is the version of firmware on the phone. For the incoming LLDPDU, the TLVs are ignored and not validated. Only one Firmware Revision TLV is allowed for the outgoing and incoming LLDPDUs.

# Final Network Policy Resolution and QoS

## Special VLANs

VLAN=0, VLAN=1, and VLAN=4095 are treated the same way as an untagged VLAN. Because the VLAN is untagged, Class of Service (CoS) is not applicable.

## Default QoS for SIP Mode

If there is no network policy from CDP or LLDP-MED, the default network policy is used. CoS is based on configuration for the specific extension. It is applicable only if the manual VLAN is enabled and manual VLAN ID is not equal to 0, 1, or 4095. Type of Service (ToS) is based on configuration for the specific extension.

## QoS Resolution for CDP

If there is a valid network policy from CDP:

- If the VLAN=0, 1, or 4095, the VLAN will not be set, or the VLAN is untagged. CoS is not applicable, but DSCP is applicable. ToS is based on the default as previously described.
- If the VLAN > 1 and VLAN < 4095, the VLAN is set accordingly. CoS and ToS are based on the default as previously described. DSCP is applicable.
- The phone reboots and restarts the fast start sequence.

## QoS Resolution for LLDP-MED

If CoS is applicable and if CoS = 0, the default is used for the specific extension as previously described. But the value shown on L2 Priority for TLV for outgoing LLDPDU is based on the value used for extension 1. If CoS is applicable and if CoS != 0, CoS is used for all extensions.

If DSCP (mapped to ToS) is applicable and if DSCP = 0, the default is used for the specific extension as previously described. But the value shown on DSCP for TLV for outgoing LLDPDU is based on value used for the extension 1. If DSCP is applicable and if DSCP != 0, DSCP is used for all extensions.

If the VLAN > 1 and VLAN < 4095, the VLAN is set accordingly. CoS and ToS are based on the default as previously described. DSCP is applicable.

If there is a valid network policy for the voice application from LLDP-MED PDU and if the tagged flag is set, the VLAN, L2 Priority (CoS), and DSCP (mapped to ToS) are all applicable.

If there is a valid network policy for the voice application from LLDP-MED PDU and if the tagged flag is not set, only the DSCP (mapped to ToS) is applicable.

The Cisco IP Phone reboots and restarts the fast start sequence.

## Coexistence with CDP

If both CDP and LLDP-MED are enabled, the network policy for the VLAN determines the last policy set or changed with either one of the discovery modes. If both LLDP-MED and CDP are enabled, during startup the phone sends CDP and LLDP-MED PDUs.

Inconsistent configuration and behavior for network connectivity devices for CDP and LLDP-MED modes could result in an oscillating rebooting behavior for the phone due to switching to different VLANs.

If the VLAN is not set by CDP and LLDP-MED, the VLAN ID that is configured manually is used. If the VLAN ID is not configured manually, no VLAN is supported. DSCP is used and the network policy determines LLDP-MED if applicable.

## LLDP-MED and Multiple Network Devices

If the same application type is used for the network policy but different Layer 2 or Layer 3 QoS Network policies are received by the phones from multiple network connectivity devices, the last valid network policy is honored. To ensure deterministic and consistent of Network Policy, multiple network connectivity devices should not send out conflicting network policies for the same application type.





# APPENDIX **B**

## TR-069 Parameter Comparison

- [XML and TR-069 Parameter Comparison, on page 467](#)

### XML and TR-069 Parameter Comparison

This table shows the XML parameters that the phones use, with their TR-069 counterpart.

TR-069 Parameter	XML Parameter
Device.Services.VoiceService.	N/A
Device.Services.VoiceService. {i}.	N/A
Device.Services.VoiceService. {i}.Capabilities.	N/A
Device.Services.VoiceService. {i}.Capabilities.ButtonMap	N/A
Device.Services.VoiceService. {i}.Capabilities.Codecs.	N/A
Device.Services.VoiceService. {i}.Capabilities.Codecs. {i}.	N/A
Device.Services.VoiceService. {i}.Capabilities.Codecs. {i}.BitRate	N/A
Device.Services.VoiceService. {i}.Capabilities.Codecs. {i}.Codec	N/A
Device.Services.VoiceService. {i}.Capabilities.Codecs. {i}.EntryID	N/A
Device.Services.VoiceService. {i}.Capabilities.Codecs. {i}.PacketizationPeriod	N/A
Device.Services.VoiceService. {i}.Capabilities.Codecs. {i}.SilenceSuppression	N/A
Device.Services.VoiceService. {i}.Capabilities.DigitMap	N/A
Device.Services.VoiceService. {i}.Capabilities.DSCPCoupled	N/A
Device.Services.VoiceService. {i}.Capabilities.EthernetTaggingCoupled	N/A
Device.Services.VoiceService. {i}.Capabilities.FaxPassThrough	N/A
Device.Services.VoiceService. {i}.Capabilities.FaxT38	N/A
Device.Services.VoiceService. {i}.Capabilities.FileBasedRingGeneration	N/A
Device.Services.VoiceService. {i}.Capabilities.FileBasedToneGeneration	N/A
Device.Services.VoiceService. {i}.Capabilities.MaxLineCount	N/A

TR-069 Parameter	XML Parameter
Device.Services.VoiceService. {i}.Capabilities.MaxProfileCount	N/A
Device.Services.VoiceService. {i}.Capabilities.MaxSessionCount	N/A
Device.Services.VoiceService. {i}.Capabilities.MaxSessionsPerLine	N/A
Device.Services.VoiceService. {i}.Capabilities.ModemPassThrough	N/A
Device.Services.VoiceService. {i}.Capabilities.NumberingPlan	N/A
Device.Services.VoiceService. {i}.Capabilities.PatternBasedRingGeneration	N/A
Device.Services.VoiceService. {i}.Capabilities.PatternBasedToneGeneration	N/A
Device.Services.VoiceService. {i}.Capabilities.PSTNSoftSwitchOver	N/A
Device.Services.VoiceService. {i}.Capabilities.Regions	N/A
Device.Services.VoiceService. {i}.Capabilities.RingDescriptionsEditable	N/A
Device.Services.VoiceService. {i}.Capabilities.RingFileFormats	N/A
Device.Services.VoiceService. {i}.Capabilities.RingGeneration	N/A
Device.Services.VoiceService. {i}.Capabilities.RingPatternEditable	N/A
Device.Services.VoiceService. {i}.Capabilities.RTCP	N/A
Device.Services.VoiceService. {i}.Capabilities.RTPRedundancy	N/A
Device.Services.VoiceService. {i}.Capabilities.SignalingProtocols	N/A
Device.Services.VoiceService. {i}.Capabilities.SIP.	N/A
Device.Services.VoiceService. {i}.Capabilities.SIP.EventSubscription	N/A
Device.Services.VoiceService. {i}.Capabilities.SIP.Extensions	N/A
Device.Services.VoiceService. {i}.Capabilities.SIP.ResponseMap	N/A
Device.Services.VoiceService. {i}.Capabilities.SIP.Role	N/A
Device.Services.VoiceService. {i}.Capabilities.SIP.TLSAuthenticationKeySizes	N/A
Device.Services.VoiceService. {i}.Capabilities.SIP.TLSAuthenticationProtocols	N/A
Device.Services.VoiceService. {i}.Capabilities.SIP.TLSEncryptionKeySizes	N/A
Device.Services.VoiceService. {i}.Capabilities.SIP.TLSEncryptionProtocols	N/A
Device.Services.VoiceService. {i}.Capabilities.SIP.TLSKeyExchangeProtocols	N/A
Device.Services.VoiceService. {i}.Capabilities.SIP.Transports	N/A
Device.Services.VoiceService. {i}.Capabilities.SIP.URISchemes	N/A
Device.Services.VoiceService. {i}.Capabilities.SRTP	N/A
Device.Services.VoiceService. {i}.Capabilities.SRTPEncryptionKeySizes	N/A
Device.Services.VoiceService. {i}.Capabilities.SRTPKeyingMethods	N/A
Device.Services.VoiceService. {i}.Capabilities.ToneDescriptionsEditable	N/A

TR-069 Parameter	XML Parameter
Device.Services.VoiceService. {i}.Capabilities.ToneFileFormats	N/A
Device.Services.VoiceService. {i}.Capabilities.ToneGeneration	N/A
Device.Services.VoiceService. {i}.Capabilities.VoicePortTests	N/A
Device.Services.VoiceService. {i}.VoiceProfile.	
Device.Services.VoiceService. {i}.VoiceProfile. {i}.	
Device.Services.VoiceService. {i}.VoiceProfile. {i}.DTMFMethod	DTMF_Tx_Method_<i>_
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Enable	N/A
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line.	
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.	
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.CallingFeatures.	
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.CallingFeatures.AnonymousCalEnable	Block_CID_Setting
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.CallingFeatures.AnonymousCallBlockEnable	
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.CallingFeatures.CallerIDEnable	Block_CID_Setting
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.CallingFeatures.CallerIDName	Display_Name_<i>_
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.CallingFeatures.CallForwardOnBusyNumber	
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.CallingFeatures.CallForwardOnNoAnswerNumber	
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.CallingFeatures.CallForwardOnNoAnswerRingCount	
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.CallingFeatures.CallForwardUnconditionalEnable	
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.CallingFeatures.CallForwardUnconditionalNumber	
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.CallingFeatures.CallReturnEnable	N/A
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.CallingFeatures.CallTransferEnable	N/A
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.CallingFeatures.CallWaitingEnable	CW_Setting
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.CallingFeatures.ConferenceCallingSessionCount	
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.CallingFeatures.ConferenceCallingStatus	N/A
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.CallingFeatures.DoNotDisturbEnable	DND_Setting
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.CallingFeatures.MaxSessions	Call_Appearances_Per_Line
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.CallingFeatures.MessageWaiting	Message_Waiting_<i>_
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.CallingFeatures.MWIEnable	N/A
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.CallingFeatures.RepeatDialEnable	N/A
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.CallingFeatures.X_CISCO_SharedLineDNDCfwdEnable	Shared_Line_DND_Cfwd_Enable
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.CallState	N/A

TR-069 Parameter	XML Parameter
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.Codec.	
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.Codec.List.	
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.Codec.List. {i}.	
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.Codec.List. {i}.BitRate	N/A
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.Codec.List. {i}.Codec	N/A
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.Codec.List. {i}.Enable	N/A
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.Codec.List. {i}.EntryID	N/A
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.Codec.List. {i}.PacketizationPeriod	N/A
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.Codec.List. {i}.Priority	
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.Codec.List. {i}.SilenceSuppression	Silence_Supp_Enable_<i>_
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.Codec.ReceiveBitRate	N/A
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.Codec.ReceiveCodec	N/A
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.Codec.ReceiveSilenceSuppression	N/A
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.Codec.TransmitBitRate	N/A
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.Codec.TransmitCodec	N/A
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.Codec.TransmitPacketizationPeriod	N/A
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.Codec.TransmitSilenceSuppression	N/A
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.Codec.X_CISCO_PREFERRED_CODEC	Preferred_Codec_<i>_
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.Codec.X_CISCO_PREFERRED_CODEC2	Second_PREFERRED_Codec_<i>_
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.Codec.X_CISCO_PREFERRED_CODEC3	Third_PREFERRED_Codec_<i>_
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.Codec.X_CISCO_USE_PREF_CODEC_ONLY	Use_Pref_Codec_Only_<i>_
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.Codec.X_CISCO_CODEC_NEGOTIATION	Codec_Negotiation_<i>_
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.DirectoryNumber	User_ID_<i>_
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.Enable	Line_Enable_<i>_
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.PhyReferenceList	N/A
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.RingMuteStatus	N/A
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.RingVolumeStatus	
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.Session.	
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.Session. {i}.	
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.Session. {i}.FarEndIPAddress	
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.Session. {i}.FarEndUDPPort	
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.Session. {i}.LocalUDPPort	



TR-069 Parameter	XML Parameter
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.Session. {i}.SessionDuration	
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.Session. {i}.SessionStartTime	
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.SIP.	
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.SIP.AuthPassword	Password_<i>_
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.SIP.AuthUserName	User_ID_<i>_
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.SIP.SIPEventSubscribeNumberOfElements	N/A
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.SIP.URI	SIP_URI_<i>_
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.SIP.X_CISCO_AuthID	Auth_ID_<i>_
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.SIP.X_CISCO_DisplayName	Display_Name_<i>_
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.SIP.X_CISCO_UseDNSSRV	Use_DNS_SRV_<i>_
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.SIP.X_CISCO_UserEqualPhone	User_Equal_Phone_<i>_
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.SIP.X_CISCO_SetG729annexb	Set_G729_annexb_<i>_
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.SIP.X_CISCO_BlindAttnXferEnable	Blind_Attn-Xfer_Enable_<i>_
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.SIP.X_CISCO_FeatureKeySync	Feature_Key_Sync_<i>_
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.SIP.X_CISCO_DNSSRVAutoPrefix	DNS_SRV_Auto_Prefix_<i>_
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.Status	N/A
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.VoiceProcessing.	N/A
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.VoiceProcessing.EchoCancellationEnable	N/A
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.VoiceProcessing.EchoCancellationInUse	N/A
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.VoiceProcessing.EchoCancellationTail	N/A
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.X_CISCO_DialPlan	Dial_Plan_<i>_
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Line. {i}.X_CISCO_DefaultRing	Default_Ring_<i>_
Device.Services.VoiceService. {i}.VoiceProfile. {i}.MaxSessions	Call_Appearences_Per_Line
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Name	N/A
Device.Services.VoiceService. {i}.VoiceProfile. {i}.NumberOfLines	N/A
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Region	N/A
Device.Services.VoiceService. {i}.VoiceProfile. {i}.Reset	N/A
Device.Services.VoiceService. {i}.VoiceProfile. {i}.RTP.	
Device.Services.VoiceService. {i}.VoiceProfile. {i}.RTP.DSCPMark	RTP_TOS_DiffServ_Value_<i>_
Device.Services.VoiceService. {i}.VoiceProfile. {i}.RTP.LocalPortMax	RTP_Port_Max
Device.Services.VoiceService. {i}.VoiceProfile. {i}.RTP.LocalPortMin	RTP_Port_Min
Device.Services.VoiceService. {i}.VoiceProfile. {i}.RTP.RTCP.	

TR-069 Parameter	XML Parameter
Device.Services.VoiceService. {i}.VoiceProfile. {i}.RTP.RTCP.Enable	RTCP_Tx_Interval
Device.Services.VoiceService. {i}.VoiceProfile. {i}.RTP.RTCP.TxRepeatInterval	RTCP_Tx_Interval
Device.Services.VoiceService. {i}.VoiceProfile. {i}.RTP.SRTP.	
Device.Services.VoiceService. {i}.VoiceProfile. {i}.RTP.SRTP.Enable	N/A
Device.Services.VoiceService. {i}.VoiceProfile. {i}.RTP.SRTP.EncryptionKeySizes	N/A
Device.Services.VoiceService. {i}.VoiceProfile. {i}.RTP.SRTP.KeyingMethods	N/A
Device.Services.VoiceService. {i}.VoiceProfile. {i}.RTP.TelephoneEventPayloadType	AVT_Dynamic_Payload
Device.Services.VoiceService. {i}.VoiceProfile. {i}.RTP.X_CISCO_RTTPPacketSize	RTP_Packet_Size
Device.Services.VoiceService. {i}.VoiceProfile. {i}.RTP.X_CISCO_RTTPBeforeACK	RTP_Before_ACK
Device.Services.VoiceService. {i}.VoiceProfile. {i}.ServiceProviderInfo.	N/A
Device.Services.VoiceService. {i}.VoiceProfile. {i}.ServiceProviderInfo.ContactPhoneNumber	N/A
Device.Services.VoiceService. {i}.VoiceProfile. {i}.ServiceProviderInfo.EmailAddress	N/A
Device.Services.VoiceService. {i}.VoiceProfile. {i}.ServiceProviderInfo.Name	N/A
Device.Services.VoiceService. {i}.VoiceProfile. {i}.ServiceProviderInfo.URL	N/A
Device.Services.VoiceService. {i}.VoiceProfile. {i}.SignalingProtocol	N/A
Device.Services.VoiceService. {i}.VoiceProfile. {i}.SIP.	
Device.Services.VoiceService. {i}.VoiceProfile. {i}.SIP.DSCPMark	SIP_TOS_DiffServ_Value_<i>_
Device.Services.VoiceService. {i}.VoiceProfile. {i}.SIP.InviteExpires	INVITE_Expires
Device.Services.VoiceService. {i}.VoiceProfile. {i}.SIP.Organization	N/A
Device.Services.VoiceService. {i}.VoiceProfile. {i}.SIP.OutboundProxy	Outbound_Proxy_<i>_
Device.Services.VoiceService. {i}.VoiceProfile. {i}.SIP.OutboundProxyPort	Outbound_Proxy_<i>_
Device.Services.VoiceService. {i}.VoiceProfile. {i}.SIP.ProxyServer	Proxy_<i>_
Device.Services.VoiceService. {i}.VoiceProfile. {i}.SIP.ProxyServerPort	Proxy_<i>_
Device.Services.VoiceService. {i}.VoiceProfile. {i}.SIP.ProxyServerTransport	SIP_Transport_<1>_
Device.Services.VoiceService. {i}.VoiceProfile. {i}.SIP.RegisterExpires	Register_Expires_<i>_
Device.Services.VoiceService. {i}.VoiceProfile. {i}.SIP.RegisterRetryInterval	Reg_Retry_Intvl
Device.Services.VoiceService. {i}.VoiceProfile. {i}.SIP.RegistersMinExpires	Reg_Min_Expires
Device.Services.VoiceService. {i}.VoiceProfile. {i}.SIP.ReInviteExpires	ReINVITE_Expires
Device.Services.VoiceService. {i}.VoiceProfile. {i}.SIP.SIPEventSubscribeNumberOfElements	N/A
Device.Services.VoiceService. {i}.VoiceProfile. {i}.SIP.SIPResponseMapNumberOfElements	N/A
Device.Services.VoiceService. {i}.VoiceProfile. {i}.SIP.TimerB	SIP_Timer_B
Device.Services.VoiceService. {i}.VoiceProfile. {i}.SIP.TimerD	SIP_Timer_D

TR-069 Parameter	XML Parameter
Device.Services.VoiceService. {i}.VoiceProfile. {i}.SIP.TimerF	SIP_Timer_F
Device.Services.VoiceService. {i}.VoiceProfile. {i}.SIP.TimerH	SIP_Timer_H
Device.Services.VoiceService. {i}.VoiceProfile. {i}.SIP.TimerJ	SIP_Timer_J
Device.Services.VoiceService. {i}.VoiceProfile. {i}.SIP.TimerT1	SIP_T1
Device.Services.VoiceService. {i}.VoiceProfile. {i}.SIP.TimerT2	SIP_T2
Device.Services.VoiceService. {i}.VoiceProfile. {i}.SIP.TimerT4	SIP_T4
Device.Services.VoiceService. {i}.VoiceProfile. {i}.SIP.UserAgentDomain	N/A
Device.Services.VoiceService. {i}.VoiceProfile. {i}.SIP.UserAgentPort	SIP_Port_<1>_
Device.Services.VoiceService. {i}.VoiceProfile. {i}.SIP.UserAgentTransport	SIP_Transport_<1>_
Device.Services.VoiceService. {i}.VoiceProfile. {i}.SIP.X_CISCO_SubMinExpires	Sub_Min_Expires
Device.Services.VoiceService. {i}.VoiceProfile. {i}.SIP.X_CISCO_SubMaxExpires	Sub_Max_Expires
Device.Services.VoiceService. {i}.VoiceProfile. {i}.SIP.X_CISCO_SubRetryIntvl	Sub_Retry_Intvl
Device.Services.VoiceService. {i}.VoiceProfile. {i}.STUNEnable	STUN_Enable
Device.Services.VoiceService. {i}.VoiceProfileNumberOfEntries	N/A
Device.Services.VoiceService. {i}.X_CISCO_SIP.	
Device.Services.VoiceService. {i}.X_CISCO_SIP.G711uCodecName	G711u_Codec_Name
Device.Services.VoiceService. {i}.X_CISCO_SIP.G711aCodecName	G711a_Codec_Name
Device.Services.VoiceService. {i}.X_CISCO_SIP.G729aCodecName	G729a_Codec_Name
Device.Services.VoiceService. {i}.X_CISCO_SIP.G729bCodecName	G729b_Codec_Name
Device.Services.VoiceService. {i}.X_CISCO_SIP.G722CodecName	G722_Codec_Name
Device.Services.VoiceService. {i}.X_CISCO_SIP.G7222CodecName	G722.2_Codec_Name
Device.Services.VoiceService. {i}.X_CISCO_SIP.iLBCCodecName	iLBC_Codec_Name
Device.Services.VoiceService. {i}.X_CISCO_SIP.OPUSCodecName	OPUS_Codec_Name
Device.Services.VoiceService. {i}.X_CISCO_SIP.AVTCodecName	AVT_Codec_Name
Device.Services.VoiceService. {i}.X_CISCO_SIP.G7222BEDynamicPayload	G722.2_Dynamic_Payload
Device.Services.VoiceService. {i}.X_CISCO_SIP.G7222OADynamicPayload	G722.2_OA_Dynamic_Payload
Device.Services.VoiceService. {i}.X_CISCO_SIP.iLBC20msDynamicPayload	iLBC_Dynamic_Payload
Device.Services.VoiceService. {i}.X_CISCO_SIP.iLBC30msDynamicPayload	iLBC_30ms_Dynamic_Payload
Device.Services.VoiceService. {i}.X_CISCO_SIP.OPUSDynamicPayload	OPUS_Dynamic_Payload
Device.Services.VoiceService. {i}.X_CISCO_SIP.AVTDynamicPayload	AVT_Dynamic_Payload
Device.Services.VoiceService. {i}.X_CISCO_SIP.AVT16kHzDynamicPayload	AVT_16kHz_Dynamic_Payload
Device.Services.VoiceService. {i}.X_CISCO_SIP.AVT48kHzDynamicPayload	AVT_48kHz_Dynamic_Payload

TR-069 Parameter	XML Parameter
Device.Services.VoiceService. {i}.X_CISCO_SIP.INFOREQDynamicPayload	INFOREQ_Dynamic_Payload
Device.Services.VoiceService. {i}.X_CISCO_SIP.DisplayAnonymousFromHeader	Display_Anonymous_From_Header
Device.Services.VoiceService. {i}.X_CISCO_SIP.RedirectKeepAlive	Redirect_Keep_Alive
Device.Services.VoiceService. {i}.X_CISCO_Regional.	
Device.Services.VoiceService. {i}.X_CISCO_Regional.Tones.	
Device.Services.VoiceService. {i}.X_CISCO_Regional.Tones.DialTone	Dial_Tone
Device.Services.VoiceService. {i}.X_CISCO_Regional.Tones.OutsideDialTone	Outside_Dial_Tone
Device.Services.VoiceService. {i}.X_CISCO_Regional.Tones.PromptTone	Prompt_Tone
Device.Services.VoiceService. {i}.X_CISCO_Regional.Tones.BusyTone	Busy_Tone
Device.Services.VoiceService. {i}.X_CISCO_Regional.Tones.ReorderTone	Reorder_Tone
Device.Services.VoiceService. {i}.X_CISCO_Regional.Tones.OffHookWarningTone	Off_Hook_Warning_Tone
Device.Services.VoiceService. {i}.X_CISCO_Regional.Tones.RingBackTone	Ring_Back_Tone
Device.Services.VoiceService. {i}.X_CISCO_Regional.Tones.CallWaitingTone	Call_Waiting_Tone
Device.Services.VoiceService. {i}.X_CISCO_Regional.Tones.ConfirmTone	Confirm_Tone
Device.Services.VoiceService. {i}.X_CISCO_Regional.Tones.MWIDialTone	MWI_Dial_Tone
Device.Services.VoiceService. {i}.X_CISCO_Regional.Tones.CfwdDialTone	Cfwd_Dial_Tone
Device.Services.VoiceService. {i}.X_CISCO_Regional.Tones.HoldingTone	Holding_Tone
Device.Services.VoiceService. {i}.X_CISCO_Regional.Tones.ConferenceTone	Conference_Tone
Device.Services.VoiceService. {i}.X_CISCO_Regional.Tones.SecureCallIndicationTone	Secure_Call_Indication_Tone
Device.Services.VoiceService. {i}.X_CISCO_Regional.Tones.PageTone	Page_Tone
Device.Services.VoiceService. {i}.X_CISCO_Regional.Tones.AlertTone	Alert_Tone
Device.Services.VoiceService. {i}.X_CISCO_Regional.Tones.MuteTone	Mute_Tone
Device.Services.VoiceService. {i}.X_CISCO_Regional.Tones.UnmuteTone	Unmute_Tone
Device.Services.VoiceService. {i}.X_CISCO_Regional.Tones.SystemBeep	System_Beep
Device.Services.VoiceService. {i}.X_CISCO_Regional.Tones.CallPickupTone	Call_Pickup_Tone
Device.Services.VoiceService. {i}.X_CISCO_Regional.Cadences.	
Device.Services.VoiceService. {i}.X_CISCO_Regional.Cadences.Cadence1	Cadence_1
Device.Services.VoiceService. {i}.X_CISCO_Regional.Cadences.Cadence2	Cadence_2
Device.Services.VoiceService. {i}.X_CISCO_Regional.Cadences.Cadence3	Cadence_3
Device.Services.VoiceService. {i}.X_CISCO_Regional.Cadences.Cadence4	Cadence_4
Device.Services.VoiceService. {i}.X_CISCO_Regional.Cadences.Cadence5	Cadence_5
Device.Services.VoiceService. {i}.X_CISCO_Regional.Cadences.Cadence6	Cadence_6

TR-069 Parameter	XML Parameter
Device.Services.VoiceService. {i}.X_CISCO_Regional.Cadences.Cadence7	Cadence_7
Device.Services.VoiceService. {i}.X_CISCO_Regional.Cadences.Cadence8	Cadence_8
Device.Services.VoiceService. {i}.X_CISCO_Regional.Cadences.Cadence9	Cadence_9
Device.Services.VoiceService. {i}.X_CISCO_Regional.Cadences.	
Device.Services.VoiceService. {i}.X_CISCO_Regional.ControlTimer.ReorderDelay	Reorder_Delay
Device.Services.VoiceService. {i}.X_CISCO_Regional.ControlTimer.InterdigitLongTimer	Interdigit_Long_Timer
Device.Services.VoiceService. {i}.X_CISCO_Regional.ControlTimer.InterdigitShortTimer	Interdigit_Short_Timer
Device.Services.VoiceService. {i}.X_CISCO_AttConsole.	
Device.Services.VoiceService. {i}.X_CISCO_AttConsole.NumberOfUnits	Number_of_Units
Device.Services.VoiceService. {i}.X_CISCO_AttConsole.ServerType	
Device.Services.VoiceService. {i}.X_CISCO_AttConsole.SubscribeRetryInterval	Subscribe_Retry_Interval
Device.Services.VoiceService. {i}.X_CISCO_AttConsole.BXferOnSpeedDialEnable	Bxfer_On_Speed_Dial_Enable
Device.Services.VoiceService. {i}.X_CISCO_AttConsole.AttendantConsoleLCDContrast	Attendant_Console_LCD_Brightness
Device.Services.VoiceService. {i}.X_CISCO_AttConsole.BXferToStarcodeEnable	Bxfer_To_Starcode_Enable
Device.Services.VoiceService. {i}.X_CISCO_AttConsole.Unit.	N/A
Device.Services.VoiceService. {i}.X_CISCO_AttConsole.Unit. {i}.	N/A
Device.Services.VoiceService. {i}.X_CISCO_AttConsole.Unit. {i}.Key.	N/A
Device.Services.VoiceService. {i}.X_CISCO_AttConsole.Unit. {i}.Key. {i}.	N/A
Device.Services.VoiceService. {i}.X_CISCO_AttConsole.Unit. {i}.Key. {i}.Config	Unit_<i>_Key_<i>_
Device.Services.VoiceService. {i}.X_CISCO_AttConsole.Unit. {i}.NumberOfKey	N/A
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.	N/A
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.LineKey.	N/A
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.LineKey. {i}.	N/A
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.LineKey. {i}.ExtendedFunction	Extended_Function_<i>_
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.LineKey. {i}.Extension	Extension_<i>_
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.LineKey. {i}.ShareCallApparence	Share_Call_Apparence_<i>_
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.LineKey. {i}.ShortName	Short_Name_<i>_
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.NumberOfLineKey	N/A
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.StationName	Station_Name
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.GroupPagingScript	Group_Paging_Script
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.VoiceMailNumber	Voice_Mail_Number
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.BluetoothMode	Bluetooth_Mode

TR-069 Parameter	XML Parameter
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.Line	Line
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.Ringtone.	N/A
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.Ringtone.Ring1	Ring1
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.Ringtone.Ring2	Ring2
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.Ringtone.Ring3	Ring3
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.Ringtone.Ring4	Ring4
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.Ringtone.Ring5	Ring5
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.Ringtone.Ring6	Ring6
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.Ringtone.Ring7	Ring7
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.Ringtone.Ring8	Ring8
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.Ringtone.Ring9	Ring9
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.Ringtone.Ring10	Ring10
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.Ringtone.Ring11	Ring11
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.Ringtone.Ring12	Ring12
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.SuppServices.	N/A
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.SuppServices.ConferenceServ	Coference_Serv
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.SuppServices.AttnTransferServ	Attn_Transfer_Serv
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.SuppServices.BlindTransferServ	Blind_Transfer_Serv
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.SuppServices.DNDServ	DND_Serv
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.SuppServices.BlockANCServ	Block_ANC_Serv
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.SuppServices.BlockCIDServ	Block_CID_Serv
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.SuppServices.SecureCallServ	Secure_Call_Serv
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.SuppServices.CfwdAllServ	Cfwd_All_Serv
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.SuppServices.CfwdBusyServ	Cfwd_Busy_Serv
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.SuppServices.CfwdNoAnsServ	Cfwd_No_Ans_Serv
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.SuppServices.PagingServ	Paging_Serv
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.SuppServices.CallParkServ	Call_Park_Serv
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.SuppServices.CallPickUpServ	Call_Pick_Up_Serv
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.SuppServices.ACDLoginServ	ACD_Login_Serv
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.SuppServices.GroupCallPickUpServ	Group_Call_Pick_Up_Serv
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.SuppServices.ServiceAnncServ	Service_Annc_Serv
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.SuppServices.CallRecordingServ	Call_Recording_Serv

TR-069 Parameter	XML Parameter
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.SuppServices.ReversePhoneLookupServ	Reverse_Phone_Lookup_Serv
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.ProgramSoftkeys.	N/A
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.ProgramSoftkeys.ProgrammableSoftkeyEnable	Programmable_Softkey_Enable
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.ProgramSoftkeys.IdleKeyList	Idle_Key_List
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.ProgramSoftkeys.MissedCallKeyList	Missed_Call_Key_List
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.ProgramSoftkeys.OffHookKeyList	Off_Hook_Key_List
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.ProgramSoftkeys.DialingInputKeyList	Dialing_Input_Key_List
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.ProgramSoftkeys.ProgressingKeyList	Progressing_Key_List
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.ProgramSoftkeys.ConnectedKeyList	Connected_Key_List
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.ProgramSoftkeys.StartXferKeyList	Start-Xfer_Key_List
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.ProgramSoftkeys.StartConfKeyList	Start-Conf_Key_List
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.ProgramSoftkeys.ConferencingKeyList	Conferencing_Key_List
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.ProgramSoftkeys.ReleasingKeyList	Releasing_Key_List
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.ProgramSoftkeys.HoldKeyList	Hold_Key_List
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.ProgramSoftkeys.RingingKeyList	Ringing_Key_List
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.ProgramSoftkeys.SharedActiveKeyList	Shared_Active_Key_List
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.ProgramSoftkeys.SharedHeldKeyList	Shared_Held_Key_List
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.ProgramSoftkeys.PSK1	PSK_1
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.ProgramSoftkeys.PSK2	PSK_2
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.ProgramSoftkeys.PSK3	PSK_3
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.ProgramSoftkeys.PSK4	PSK_4
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.ProgramSoftkeys.PSK5	PSK_5
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.ProgramSoftkeys.PSK6	PSK_6
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.ProgramSoftkeys.PSK7	PSK_7
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.ProgramSoftkeys.PSK8	PSK_8
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.ProgramSoftkeys.PSK9	PSK_9
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.ProgramSoftkeys.PSK10	PSK_10
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.ProgramSoftkeys.PSK11	PSK_11
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.ProgramSoftkeys.PSK12	PSK_12
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.ProgramSoftkeys.PSK13	PSK_13
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.ProgramSoftkeys.PSK14	PSK_14
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.ProgramSoftkeys.PSK15	PSK_15

TR-069 Parameter	XML Parameter
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.ProgramSoftkeys.PSK16	PSK_16
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.LDAP.	N/A
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.LDAP.LDAPDirEnable	LDAP_Dir_Enable
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.LDAP.CorpDirName	LDAP_Corp_Dir_Name
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.LDAP.Server	LDAP_Server
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.LDAP.SearchBase	LDAP_Search_Base
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.LDAP.ClientDN	LDAP_Client_DN
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.LDAP.UserName	LDAP_User_Name
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.LDAP.Password	LDAP_Password
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.LDAP.AuthMethod	LDAP_Auth_Method
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.LDAP.LastNameFilter	LDAP_Last_Name_Filter
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.LDAP.FirstNameFilter	LDAP_First_Name_Filter
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.LDAP.SearchItem3	LDAP_Search_Item_3
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.LDAP.SearchItem3Filter	LDAP_Item_3_Filter
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.LDAP.SearchItem4	LDAP_Search_Item_4
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.LDAP.SearchItem4Filter	LDAP_Item_4_Filter
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.LDAP.DisplayAttrs	LDAP_Display_Attrs
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.LDAP.NumberMapping	LDAP_Number_Mapping
Device.Services.VoiceService. {i}.X_CISCO_PhoneSetting.LDAP.StartTLSEnable	LDAP_StartTLS_Enable
Device.Services.VoiceService. {i}.X_CISCO_UserSetting.	N/A
Device.Services.VoiceService. {i}.X_CISCO_UserSetting.RingerVolume	Ringer_Volume
Device.Services.VoiceService. {i}.X_CISCO_UserSetting.SpeakerVolume	Speaker_Volume
Device.Services.VoiceService. {i}.X_CISCO_UserSetting.HandsetVolume	Handset_Volume
Device.Services.VoiceService. {i}.X_CISCO_UserSetting.HeadsetVolume	Headset_Volume
Device.Services.VoiceService. {i}.X_CISCO_UserSetting.PhoneBackground	Phone_Background
Device.Services.VoiceService. {i}.X_CISCO_UserSetting.PictureDownloadURL	Picture_Download_URL
Device.Services.VoiceService. {i}.X_CISCO_UserSetting.ElectronicHookSwitchControl	Ehook_Enable
Device.Services.VoiceService. {i}.X_CISCO_UserSetting.ScreenSaverEnable	Screen_Saver_Enable
Device.Services.VoiceService. {i}.X_CISCO_UserSetting.ScreenSaverType	Screen_Saver_Type
Device.Services.VoiceService. {i}.X_CISCO_UserSetting.MissCallShortcut	Miss_Call_Shortcut
Device.Services.VoiceService. {i}.X_CISCO_UserSetting.AlertToneOff	Alert_Tone_Off
Device.Services.VoiceService. {i}.X_CISCO_UserSetting.LogoURL	Logo_URL



TR-069 Parameter	XML Parameter
Device.Services.VoiceService. {i}.X_CISCO_StarCode.	N/A
Device.Services.VoiceService. {i}.X_CISCO_StarCode.ActivateBlockAnonymousCall	Block_ANC_Act_Code
Device.Services.VoiceService. {i}.X_CISCO_StarCode.ActivateBlockCallerId	Block_CID_Act_Code
Device.Services.VoiceService. {i}.X_CISCO_StarCode.ActivateBlockCallerIdNextCall	Block_CID_Per_Call_Act_Code
Device.Services.VoiceService. {i}.X_CISCO_StarCode.ActivateCallForwardAll	Cfwd_All_Act_Code
Device.Services.VoiceService. {i}.X_CISCO_StarCode.ActivateCallForwardBusy	Cfwd_Busy_Act_Code
Device.Services.VoiceService. {i}.X_CISCO_StarCode.ActivateCallForwardNoAnswer	Cfwd_No_Ans_Act_Code
Device.Services.VoiceService. {i}.X_CISCO_StarCode.ActivateCallWaiting	CW_Act_Code
Device.Services.VoiceService. {i}.X_CISCO_StarCode.ActivateCallWaitingNextCall	CW_Per_Call_Act_Code
Device.Services.VoiceService. {i}.X_CISCO_StarCode.ActivateDoNotDisturb	DND_Act_Code
Device.Services.VoiceService. {i}.X_CISCO_StarCode.ActivateSecureCall	Secure_All_Call_Act_Code
Device.Services.VoiceService. {i}.X_CISCO_StarCode.ActivateSecureCallNextCall	Secure_One_Call_Act_Code
Device.Services.VoiceService. {i}.X_CISCO_StarCode.BlindTransfer	Blind_Transfer_Code
Device.Services.VoiceService. {i}.X_CISCO_StarCode.CallPark	Call_Park_Code
Device.Services.VoiceService. {i}.X_CISCO_StarCode.CallPickup	Call_Pickup_Code
Device.Services.VoiceService. {i}.X_CISCO_StarCode.CallReturn	Call_Return_Code
Device.Services.VoiceService. {i}.X_CISCO_StarCode.CallUnpark	Call_Unpark_Code
Device.Services.VoiceService. {i}.X_CISCO_StarCode.DeactivateBlockAnonymousCall	Block_ANC_Deact_Code
Device.Services.VoiceService. {i}.X_CISCO_StarCode.DeactivateBlockCallerId	Block_CID_Deact_Code
Device.Services.VoiceService. {i}.X_CISCO_StarCode.DeactivateBlockCallerIdNextCall	Block_CID_Per_Call_Deact_Code
Device.Services.VoiceService. {i}.X_CISCO_StarCode.DeactivateCallForwardAll	Cfwd_All_Deact_Code
Device.Services.VoiceService. {i}.X_CISCO_StarCode.DeactivateCallForwardBusy	Cfwd_Busy_Deact_Code
Device.Services.VoiceService. {i}.X_CISCO_StarCode.DeactivateCallForwardNoAnswer	Cfwd_No_Ans_Deact_Code
Device.Services.VoiceService. {i}.X_CISCO_StarCode.DeactivateCallWaiting	CW_Deact_Code
Device.Services.VoiceService. {i}.X_CISCO_StarCode.DeactivateCallWaitingNextCall	CW_Per_Call_Deact_Code
Device.Services.VoiceService. {i}.X_CISCO_StarCode.DeactivateDoNotDisturb	DND_Deact_Code
Device.Services.VoiceService. {i}.X_CISCO_StarCode.DeactivateSecureCal	Secure_No_Call_Act_Code
Device.Services.VoiceService. {i}.X_CISCO_StarCode.DeactivateSecureCallNextCall	Secure_One_Call_Deact_Code
Device.Services.VoiceService. {i}.X_CISCO_StarCode.GroupCallPickup	Group_Call_Pickup_Code
Device.Services.VoiceService. {i}.X_CISCO_StarCode.PagingCode	Paging_Code
Device.Services.VoiceService. {i}.X_CISCO_StarCode.PreferCodecG711a	Prefer_G711a_Code
Device.Services.VoiceService. {i}.X_CISCO_StarCode.PreferCodecG711u	Prefer_G711u_Code

TR-069 Parameter	XML Parameter
Device.Services.VoiceService. {i}.X_CISCO_StarCode.PreferCodecG722	Prefer_G722_Code
Device.Services.VoiceService. {i}.X_CISCO_StarCode.PreferCodecG7222	Prefer_G722.2_Code
Device.Services.VoiceService. {i}.X_CISCO_StarCode.PreferCodecG729a	Prefer_G729a_Code
Device.Services.VoiceService. {i}.X_CISCO_StarCode.PreferCodeciLBC	Prefer_iLBC_Code
Device.Services.VoiceService. {i}.X_CISCO_StarCode.PreferCodecOPUS	Prefer_OPUS_Code
Device.Services.VoiceService. {i}.X_CISCO_StarCode.UseOnlyCodecG711a	Force_G711a_Code
Device.Services.VoiceService. {i}.X_CISCO_StarCode.UseOnlyCodecG711u	Force_G711u_Code
Device.Services.VoiceService. {i}.X_CISCO_StarCode.UseOnlyCodecG722	Force_G722_Code
Device.Services.VoiceService. {i}.X_CISCO_StarCode.UseOnlyCodecG7222	Force_G722.2_Code
Device.Services.VoiceService. {i}.X_CISCO_StarCode.UseOnlyCodecG729a	Force_G729a_Code
Device.Services.VoiceService. {i}.X_CISCO_StarCode.UseOnlyCodeciLBC	Force_iLBC_Code
Device.Services.VoiceService. {i}.X_CISCO_StarCode.UseOnlyCodecOPUS	Force_OPUS_Code
	N/A
	N/A
*(1) We support such TR-069 configuration, but no corresponding parameter on Web/GUI	N/A
*(2) We support such TR-069 configuration, but can only be set to 'Yes'	N/A
*(3) i=0 G.711MuLaw i=1 G.711ALaw i=2 G.729a i=3 G.722 i=4 G.722.2 i=5 iLBC i=6 (88xx iSAC) (78xx OPUS) i=7 OPUS (88xx)	N/A
*(4) Only available on 8851/8861/8865	N/A
*(5) This parameter is for global setting, not per extension	N/A
*(6) This will leads to codec <i> on line <i> enable/disable, for codec <i>, please refer to *(4)	N/A
*(7) Only with sidecar. On mountlake it is named Attendant Console LCD Contrast	N/A
Device.	N/A
Device.DeviceSummary	N/A
Device.Services.	N/A
Device.Services.VoiceServiceNumberOfEntries	
Device.DeviceInfo.	N/A
Device.DeviceInfo.Manufacturer	N/A
Device.DeviceInfo.ManufacturerOUI	N/A
Device.DeviceInfo.ModelName	N/A
Device.DeviceInfo.Description	N/A

TR-069 Parameter	XML Parameter
Device.DeviceInfo.ProductClass	N/A
Device.DeviceInfo.SerialNumber	N/A
Device.DeviceInfo.HardwareVersion	N/A
Device.DeviceInfo.SoftwareVersion	N/A
Device.DeviceInfo.EnabledOptions	N/A
Device.DeviceInfo.AdditionalHardwareVersion	N/A
Device.DeviceInfo.AdditionalSoftwareVersion	N/A
Device.DeviceInfo.ProvisioningCode	N/A
Device.DeviceInfo.DeviceStatus	N/A
Device.DeviceInfo.UpTime	N/A
Device.ManagementServer.	N/A
Device.ManagementServer.URL	N/A
Device.ManagementServer.Username	N/A
Device.ManagementServer.Password	N/A
Device.ManagementServer.PeriodicInformEnable	N/A
Device.ManagementServer.PeriodicInformInterval	N/A
Device.ManagementServer.PeriodicInformTime	N/A
Device.ManagementServer.ParameterKey	N/A
Device.ManagementServer.ConnectionRequestURL	N/A
Device.ManagementServer.ConnectionRequestUsername	N/A
Device.ManagementServer.ConnectionRequestPassword	N/A
Device.GatewayInfo.	N/A
Device.GatewayInfo.ManufacturerOUI	N/A
Device.GatewayInfo.ProductClass	N/A
Device.GatewayInfo.SerialNumber	N/A
Device.Time.	N/A
Device.Time.NTPServer1	Primary_NTP_Server
Device.Time.NTPServer2	Secondary_NTP_Server
Device.Time.CurrentLocalTime	N/A
Device.Time.LocalTimeZone	Time_Zone
Device.Time.X_CISCO_TimeFormat	Time_Format
Device.Time.X_CISCO_DateFormat	Date_Format

TR-069 Parameter	XML Parameter
Device.LAN.	N/A
Device.LAN.X_CISCO_IPMode	IP_Mode
Device.LAN.AddressingType	Connection_Type
Device.LAN.IPAddress	Static_IP
Device.LAN.SubnetMask	NetMask
Device.LAN.DefaultGateway	Gateway
Device.LAN.DNSServers	Primary_DNS
Device.LAN.MACAddress	N/A
Device.LAN.DHCPOptionNumberOfEntries	N/A
Device.LAN.DHCPOption.	N/A
Device.LAN.DHCPOption. {i}.	N/A
Device.LAN.DHCPOption. {i}.Request	DHCP_Option_To_Use
Device.LAN.DHCPOption. {i}.Tag	DHCP_Option_To_Use
Device.LAN.DHCPOption. {i}.Value	DHCP_Option_To_Use
Device.Ethernet.	N/A
Device.Ethernet.X_CISCO_CDP	Enable_CDP
Device.Ethernet.X_CISCO_LLDP	Enable_LLDP-MED
Device.Ethernet.X_CISCO_EnableVLAN	Enable_VLAN
Device.Ethernet.X_CISCO_VLANID	VLAN_ID
Device.X_CISCO_Language.	N/A
Device.X_CISCO_Language.DictionaryServerScript	Dictionary_Server_Script
Device.X_CISCO_Language.LanguageSelection	Language_Selection
Device.X_CISCO_Language.Locale	Locale
Device.X_CISCO_XmlService.	N/A
Device.X_CISCO_SecuritySettings.TLSCipherList	TLS_Cipher_List
Device.X_CISCO_XmlService.Password	XML_Password
Device.X_CISCO_XmlService.UserName	XML_User_Name
Device.X_CISCO_XmlService.XMLAppServiceName	XML_Application_Service_Name
Device.X_CISCO_XmlService.XMLAppServiceURL	XML_Application_Service_URL
Device.X_CISCO_XmlService.XMLDirServiceName	XML_Directory_Service_Name
Device.X_CISCO_XmlService.XMLDirServiceURL	XML_Directory_Service_URL
Device.X_CISCO_XmlService.CISCOXMLEXEEnable	CISCO_XML_EXE_Enable

<b>TR-069 Parameter</b>	<b>XML Parameter</b>
Device.X_CISCO_XmlService.CISCOXML_EXE_AUTH_MODE	CISCO_XML_EXE_AUTH_MODE
Device.X_CISCO_RestrictedAccessDomains	Restricted_Access_Domains
Device.X_CISCO_EnableWebServer	Enable_Web_Server
Device.X_CISCO_WebProtocol	Enable_Protocol
Device.X_CISCO_EnableDirectActionUrl	Enable_Direct_Action_Url
Device.X_CISCO_SessionMaxTimeout	Session_Max_Timeout
Device.X_CISCO_SessionIdleTimeout	Session_Idle_Timeout
Device.X_CISCO_WebServerPort	Web_Server_Port
Device.X_CISCO_EnableWebAdminAccess	Enable_Web_Admin_Access
Device.X_CISCO_HostName	Host_Name
Device.X_CISCO_Domain	Domain
Device.X_CISCO_UpgradeErrorRetryDelay	Upgrade_Error_Retry_Delay
Device.X_CISCO_UpgradeRule	Upgrade_Rule
Device.X_CISCO_ProfileRule	Profile_Rule
Device.X_CISCO_UserConfigurableResync	User_Configurable_Resync
Device.X_CISCO_HTTPReportMethod	HTTP_Report_Method
Device.X_CISCO_CWMPV1dot2Support	CWMP_V1.2_Support

