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 HEREBIN, 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.

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: http://www.cisco.com/go/trademarks. 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. (1110R)

© 2018 Cisco Systems, Inc. All rights reserved.
CONTENTS

Preface xv
  Overview xv
  Audience xv
  Organization xvi
Related Documentation xvii
  Cisco Unified IP Phone 7900 Series Documentation xvii
  Cisco Unified Communications Manager Documentation xvii
  Cisco Business Edition 5000 Documentation xvii
Documentation, Support, and Security Guidelines xvii
Cisco Product Security Overview xvii
Guide Conventions xviii

CHAPTER 1 Cisco Unified IP Phone 1
  Phone Overview 1
  Cisco Unified IP Phone 7975G, 7971G-GE, 7970G, 7965G, and 7945G Components 2
    Cisco Unified IP Phone 7975G Buttons and Hardware 2
    Cisco Unified IP Phone 7970G and 7971G-GE Buttons and Hardware 2
    Cisco Unified IP Phone 7965G Buttons and Hardware 3
    Cisco Unified IP Phone 7945G Buttons and Hardware 3
    Buttons and Hardware Identification 4
  Network Protocols 6
    IPv6 Support on Cisco Unified IP Phones 11
  Cisco Unified IP Phone 7975G, 7971G-GE, 7970G, 7965G, and 7945G Supported Features 11
    Feature Overview 11
    Telephony Feature Administration 12
    Cisco Unified IP Phone Network Parameters 12
    Information for End Users 13
Cisco Unified IP Phone Security Features 13

Supported Security Features 15

Security Profiles 17

Authenticated, Encrypted, and Protected Phone Calls 18

Secure Conference Call Identification 18

Protected Call Identification 19

Call Security Interactions and Restrictions 19

802.1X Authentication 21

Overview 21

Required Network Components 22

Best-Practice Requirements and Recommendations 22

Security Restrictions 23

Phone Power Consumption 23

Cisco Unified IP Phone Deployment 23

Cisco Unified IP Phone Setup in Cisco Unified Communications Manager 24

Set Up Cisco Unified IP Phone 7975G, 7971G-GE, 7970G, 7965G, and 7945G in Cisco Unified Communications Manager Administration 24

Cisco Unified IP Phone Installation 26

Install Cisco Unified IP Phone 7975G, 7971G-GE, 7970G, 7965G, and 7945G 26

CHAPTER 2

Cisco Unified IP Phones and Telephony Networks 29

Phone and Telephony Network Overview 29

Cisco Unified IP Communications Product Interactions 29

Cisco Unified IP Phone and Cisco Unified Communications Manager Interactions 30

Cisco Unified IP Phone and VLAN Interaction 30

Cisco Unified IP Phone Power 31

Power Guidelines 31

Phone Power Consumption and Display Brightness 32

Power Outage 34

Additional Information About Power 34

Phone Configuration Files 34

Phone Startup Process 36

Cisco Unified Communications Manager Phone Addition Methods 37

Autoregistration Phone Addition 38

Autoregistration and TAPS Phone Addition 39
CHAPTER 3 Cisco Unified IP Phones Installation 43

Phone Installation Overview 43
Before You Begin 43
Network Requirements 44
Cisco Unified Communications Manager Setup 44
Cisco Unified IP Phone Components 44
Network and Access Ports 45
Handset 45
Speakerphone 45
  Disable Speakerphone 46
Headset 46
  Audio Quality 46
  Headset Connection 47
  Disable Headset 47
  Wireless Headset 47
  Enable Headset Hookswitch Control 48
  External Device Use 48
Install Cisco Unified IP Phone 48
  Cisco Unified IP Phone Cable Installation 49
Cisco Unified IP Phone Expansion Module 50
  Set up Cisco Unified IP Phone Expansion Module 51
  Feature Key Capacity Increase for Cisco Unified IP Phones 52
  Set up Additional Buttons 53
Footstand Adjustment 53
Phone Cable Lock 53
  Cisco Unified IP Phones 7945G, 7965G, and 7975G Cable Lock 54
  Cisco Unified IP Phones 7970G and 7971G-GE Cable Lock 55
Mount Phone on Wall  55
Phone Startup Process  57
Network Settings  58
Cisco Unified IP Phone Security  58
Supported TLS and Ciphers  58
Install Locally Significant Certificate  59

CHAPTER 4
Cisco Unified IP Phone Settings  61
Phone Settings Overview  61
Cisco Unified IP Phone Menus  61
  Display Settings Menu  62
  Unlock and Lock Options  63
  Value Input Guidelines  63
Phone Setup Options  64
Network Configuration Menu  66
  Set IPv4 Configuration Fields  75
  Set IPv6 Configuration Fields  76
  Set Domain Name Field  76
  Set Admin VLAN ID Field  77
  Set SW Port Configuration Field  77
  Set PC Port Configuration Field  77
  Set PC VLAN Field  78
  Set DHCP Field  78
  Set IP Address Field  78
  Set Subnet Mask Field  79
  Set Default Router Fields  79
  Set DNS Server Fields  79
  Set DHCP Address Released Field  80
  Set Alternate TFTP Field  80
  Set TFTP Server 1 Field  80
  Set TFTP Server 2 Field  81
  Set DHCPv6 Field  81
  Set IPv6 Address Field  81
  Set IPv6 Prefix Length Field  82
  Set IPv6 Default Router 1 Field  82
Set IPv6 DNS Server 1 and IPv6 DNS Server 2 Fields 82
Set DHCPv6 Address Released Field 83
Set IPv6 Alternate TFTP Field 83
Set IPv6 TFTP Server 1 Field 83
Set IPv6 TFTP Server 2 Field 84
DHCPv6 and Autoconfiguration 84
Device Configuration Menu 85
Unified CM Configuration Menu 85
SIP Configuration Menu for SIP Phones 87
SIP General Configuration Menu 87
Line Settings Menu for SIP Phones 88
Call Preferences Menu for SIP Phones 89
HTTP Configuration Menu 90
Locale Configuration Menu 92
NTP Configuration Menu for SIP Phones 93
UI Configuration Menu 93
Media Configuration Menu 96
Power Save Configuration Menu 99
Ethernet Configuration Menu 100
Security Configuration Menu 101
QoS Configuration Menu 102
Network Configuration Menu 103
Security Configuration Menu 109
CTL File Submenu 111
Unlock CTL and ITL Files 113
ITL File Submenu 113
Trust List Menu 115
802.1X Authentication and Status Menus 116
Set Device Authentication Field 118
Set EAP-MD5 Shared Secret Field 118
VPN Configuration Menu 119
Connect to VPN 119
VPN Configuration Fields 120

CHAPTER 5 Features, Templates, Services, and Users 123
CHAPTER 6

Cisco Unified IP Phone Customization 167

Configuration File Customization and Modification 167

Custom Phone Ring Creation 168
  Ringlist.xml File Format Requirements 168
  PCM File Requirements for Custom Ring Types 169
  Set Up Custom Phone Ring 169
Custom Background Images 170
List.xml File Format Requirements 170
PNG File Requirements for Custom Background Images 171
Set Up Custom Background Image 171
Wideband Codec Setup 172
Idle Display Setup 173
Cisco Unified IP Phone Backlight 174

CHAPTER 7
Model Information, Status, and Statistics 177
Model Information, Status, and Statistics Overview 177
Display Model Information Screen 178
Model Information Settings 178
Status Menu 179
Display Status Menu 179
Status Messages Screen 179
Status Messages Screen 179
Status Messages 180
Network Statistics Screen 188
Display Network Statistics Screen 188
Network Statistics Items 188
Firmware Version Screen 191
Display Firmware Version Screen 191
Firmware Version Items 192
Expansion Modules Screen 192
Display Expansion Modules Screen 192
Expansion Module Items 193
Call Statistics Screen 193
Display Call Statistics Screen 194
Call Statistics Items 194
Test Tone 196
Enable Tone Generator 196
Create Test Tone 197

CHAPTER 8
Remote Monitoring 199
Remote Monitoring Overview 199
Troubleshooting and Maintenance 217

Troubleshooting and Maintenance Overview 217

Troubleshooting 217

Startup Problems 217

Cisco Unified IP Phone Does Not Go Through Normal Startup Process 217

Cisco Unified IP Phone Does Not Register with Cisco Unified Communications Manager 218

Phone Displays Error Messages 219

Phone Cannot Connect to TFTP Server or to Cisco Unified Communications Manager 219

TFTP Server Settings 219

IP Addressing and Routing 219

DNS Settings 219

Cisco Unified Communications Manager Settings on Phone 220

Cisco CallManager and TFTP Services Are Not Running 220

Configuration File Corruption 220

Cisco Unified Communications Manager Phone Registration 220

Cisco Unified IP Phone Cannot Obtain IP Address 221

Cisco Unified IP Phone Displays Security Error Message 221

Cisco Unified IP Phone Resets Unexpectedly 222

Physical Connection Problems 222

Intermittent Network Outages 222

DHCP Setting Errors 222
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static IP Address Setting Errors</td>
<td>223</td>
</tr>
<tr>
<td>Voice VLAN Setup Errors</td>
<td>223</td>
</tr>
<tr>
<td>Phones Have Not Been Intentionally Reset</td>
<td>223</td>
</tr>
<tr>
<td>DNS or Other Connectivity Errors</td>
<td>224</td>
</tr>
<tr>
<td>Power Connection Problems</td>
<td>224</td>
</tr>
<tr>
<td>Cisco Unified IP Phone Security Problems</td>
<td>224</td>
</tr>
<tr>
<td>CTL File Problems</td>
<td>224</td>
</tr>
<tr>
<td>Authentication Error, Phone Cannot Authenticate CTL File</td>
<td>224</td>
</tr>
<tr>
<td>Phone Cannot Authenticate CTL File</td>
<td>225</td>
</tr>
<tr>
<td>ITL File Authenticates but Other Configuration Files Do Not Authenticate</td>
<td>225</td>
</tr>
<tr>
<td>Phone Does Not Register</td>
<td>225</td>
</tr>
<tr>
<td>Signed Configuration Files Are Not Requested</td>
<td>225</td>
</tr>
<tr>
<td>802.1X Authentication Problems</td>
<td>226</td>
</tr>
<tr>
<td>802.1X Enabled on Phone but Phone Does Not Authenticate</td>
<td>227</td>
</tr>
<tr>
<td>802.1X Not Enabled</td>
<td>227</td>
</tr>
<tr>
<td>Factory Reset of Phone Has Deleted 802.1X Shared Secret</td>
<td>228</td>
</tr>
<tr>
<td>Audio and Video Problems</td>
<td>228</td>
</tr>
<tr>
<td>Phone Display Is Wavy</td>
<td>228</td>
</tr>
<tr>
<td>No Speech Path</td>
<td>228</td>
</tr>
<tr>
<td>General Telephone Call Problems</td>
<td>229</td>
</tr>
<tr>
<td>VPN-Connected Phone Does Not Log Calls</td>
<td>229</td>
</tr>
<tr>
<td>Phone Does Not Recognize DTMF Digits or Digits Are Delayed</td>
<td>229</td>
</tr>
<tr>
<td>Troubleshooting Procedures</td>
<td>229</td>
</tr>
<tr>
<td>Set Up Remote Phone</td>
<td>230</td>
</tr>
<tr>
<td>Check TFTP Settings</td>
<td>230</td>
</tr>
<tr>
<td>Check DHCP settings</td>
<td>230</td>
</tr>
<tr>
<td>Verify DNS Settings</td>
<td>231</td>
</tr>
<tr>
<td>Create New Phone Configuration File</td>
<td>231</td>
</tr>
<tr>
<td>Start Service</td>
<td>232</td>
</tr>
<tr>
<td>Determine DNS or Connectivity Issues</td>
<td>233</td>
</tr>
<tr>
<td>General Troubleshooting Information</td>
<td>233</td>
</tr>
<tr>
<td>General Troubleshooting Tips for Cisco Unified IP Phone Expansion Module</td>
<td>236</td>
</tr>
<tr>
<td>Cisco Unified IP Phone Reset or Restore</td>
<td>236</td>
</tr>
<tr>
<td>Basic Reset</td>
<td>237</td>
</tr>
<tr>
<td>Factory Reset</td>
<td>237</td>
</tr>
</tbody>
</table>
Additional Troubleshooting Information 238
Maintenance 238
Quality Report Tool 239
Voice Quality Monitoring 239
Voice Quality Metric Interpretation 240
Voice Quality Troubleshooting Tips 240
Cisco Unified IP Phone Cleaning 241

APPENDIX A

Internal Support Web Site 243
Internal Support Web Site Overview 243
Cisco Unified IP Phone User Support 243
User Options Web Pages Access 244
Online Help on Phone 244
Cisco Unified IP Phone Manuals 244
Cisco Unified IP Phone 7900 Series eLearning Tutorials for SCCP Phones 245
Phone Features User Subscription and Setup 245
User Voice Messaging System Access 246
User Personal Directory Entries Setup 246
Obtain Cisco Unified IP Phone Address Book Synchronizer 246
Cisco Unified IP Phone Address Book Synchronizer Deployment 247
Install Synchronizer 247
Set Up Synchronizer 247

APPENDIX B

Feature Support by Protocol for Cisco Unified IP Phones 249

APPENDIX C

International User Support 259
International User Support Overview 259
Language Overlays for Phone Buttons 259
Unified Communications Manager Endpoints Locale Installer 259
Language Limitation 260
International Call Logging Support 260

APPENDIX D

Technical Specifications 261
Physical and Operating Environment Specifications 261
Cable Specifications 263
Preface

Overview, page xv
Audience, page xv
Organization, page xvi
Related Documentation, page xvii
Documentation, Support, and Security Guidelines, page xvii
Cisco Product Security Overview, page xvii
Guide Conventions, page xviii

Overview

Cisco Unified IP Phone 7975G, 7971G-GE, 7970G, 7965G, and 7945G Administration Guide for Cisco Unified Communications Manager (SCCP and SIP) provides the information you need to understand, install, configure, manage, and troubleshoot the Cisco Unified IP Phone on a Voice-over-IP (VoIP) network.

Because of the complexity of a Unified Communications network, this guide does not provide complete and detailed information for procedures that you need to perform in Cisco Unified Communications Manager (formerly Cisco Unified CallManager) or on other network devices.

Related Topics
Related Documentation, on page xvii

Audience

Network engineers, system administrators, and telecom engineers should review this guide to learn the steps that are required to set up Cisco Unified IP Phones. The tasks described in this document involve configuring network settings that are not intended for phone users. The tasks in this manual require a familiarity with Cisco Unified Communications Manager.
This manual is organized as follows:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified IP Phone, on page 1</td>
<td>Provides a conceptual overview and description of the Cisco Unified IP Phone.</td>
</tr>
<tr>
<td>Cisco Unified IP Phones and Telephony Networks, on page 29</td>
<td>Describes how the Cisco Unified IP Phone interacts with other key IP telephony components, and provides an overview of the tasks that are required prior to installation.</td>
</tr>
<tr>
<td>Cisco Unified IP Phones Installation, on page 43</td>
<td>Describes how to properly and safely install and configure the Cisco Unified IP Phone on your network.</td>
</tr>
<tr>
<td>Cisco Unified IP Phone Settings, on page 61</td>
<td>Describes how to configure network settings, verify status, and make global changes to the Cisco Unified IP Phone.</td>
</tr>
<tr>
<td>Features, Templates, Services, and Users, on page 123</td>
<td>Provides an overview of procedures to configure telephony features, configure directories, configure phone button and softkey templates, set up services, and add users to Cisco Unified Communications Manager.</td>
</tr>
<tr>
<td>Cisco Unified IP Phone Customization, on page 167</td>
<td>Explains how to customize phone ring sounds, background images, and the phone idle display at your site.</td>
</tr>
<tr>
<td>Model Information, Status, and Statistics, on page 177</td>
<td>Explains how to view model information, status messages, network statistics, and firmware information from the Cisco Unified IP Phone.</td>
</tr>
<tr>
<td>Remote Monitoring, on page 199</td>
<td>Describes the information that you can obtain from the phone web page, and how to use this information to monitor the operation of a phone remotely and to assist with troubleshooting.</td>
</tr>
<tr>
<td>Troubleshooting and Maintenance, on page 217</td>
<td>Provides tips for troubleshooting the Cisco Unified IP Phone.</td>
</tr>
<tr>
<td>Internal Support Web Site, on page 243</td>
<td>Provides suggestions for setup of a website that provides users with important information about their Cisco Unified IP Phones.</td>
</tr>
<tr>
<td>Feature Support by Protocol for Cisco Unified IP Phones, on page 249</td>
<td>Provides information about feature support for the Cisco Unified IP Phone that uses the SCCP or SIP protocol.</td>
</tr>
<tr>
<td>International User Support, on page 259</td>
<td>Provides information about phone setup in non-English environments.</td>
</tr>
<tr>
<td>Technical Specifications, on page 261</td>
<td>Provides technical specifications of the Cisco Unified IP Phone.</td>
</tr>
<tr>
<td>Basic Phone Administration Steps, on page 265</td>
<td>Provides procedures for basic administration tasks, such as adding a user and phone to Cisco Unified Communications Manager and then associating the user to the phone.</td>
</tr>
</tbody>
</table>
Related Documentation

Use the following sections to obtain related information.

Cisco Unified IP Phone 7900 Series Documentation

See the publications that are specific to your language, phone model, and Cisco Unified Communications Manager release. Navigate from the following documentation URL:


Cisco Unified Communications Manager Documentation

See the *Cisco Unified Communications Manager Documentation Guide* and other publications that are specific to your Cisco Unified Communications Manager release. Navigate from the following documentation URL:


Cisco Business Edition 5000 Documentation

See the *Cisco Business Edition 5000 Documentation Guide* and other publications that are specific to your Cisco Business Edition 5000 release. Navigate from the following URL:


Documentation, Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, reviewing security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What’s New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:


Subscribe to the *What’s New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

Cisco Product Security Overview

This product contains cryptographic features and is subject to United States and local country laws governing 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 may be found at http://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear.

Guide Conventions

This document uses the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>boldface</strong> font</td>
<td>Commands and keywords are in <strong>boldface</strong>.</td>
</tr>
<tr>
<td><em>italic</em> font</td>
<td>Arguments for which you supply values are in <em>italics</em>.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Elements in square brackets are optional.</td>
</tr>
<tr>
<td>{ x</td>
<td>y</td>
</tr>
<tr>
<td>[ x</td>
<td>y</td>
</tr>
<tr>
<td>string</td>
<td>A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.</td>
</tr>
<tr>
<td><strong>screen</strong> font</td>
<td>Terminal sessions and information the system displays are in <strong>screen</strong> font.</td>
</tr>
<tr>
<td><strong>input</strong> font</td>
<td>Information you must enter is in <strong>input</strong> font.</td>
</tr>
<tr>
<td><em>italic screen</em> font</td>
<td>Arguments for which you supply values are in <em>italic screen</em> font.</td>
</tr>
<tr>
<td>^</td>
<td>The symbol ^ represents the key labeled Control - for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.</td>
</tr>
<tr>
<td>&lt; &gt;</td>
<td>Nonprinting characters such as passwords are in angle brackets.</td>
</tr>
</tbody>
</table>

**Note**

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

**Caution**

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Warnings use the following convention:
IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS
Cisco Unified IP Phone

Phone Overview

The Cisco Unified IP Phone 7975G, 7971G-GE, 7970G, 7965G, and 7945G is a full-featured telephone that provides voice communication over an Internet Protocol (IP) network. These IP phones function much like digital business phones and allow you to place and receive phone calls and to access features such as mute, hold, transfer, speed dial, call forward, and more. In addition, because Cisco Unified IP Phones connect to your data network, they offer enhanced IP telephony features, such as access to network information and services and customizable features and services. The phones also support security features that include file authentication, device authentication, signaling encryption, and media encryption.

The Cisco Unified IP Phone 7975G, 7971G-GE, 7970G, 7965G, and 7945G provides a color screen (touchscreen for the 7975G, 7971G-GE, and the 7970G), support for line or speed dial numbers, context-sensitive online help for buttons and features, and a variety of other sophisticated functions.

A Cisco Unified IP Phone, like other network devices, must be configured and managed. These phones encode G.711a, G.711mu, G.722, G.729a, G.729ab, iLBC, and decode G.711a, G.711mu, G.722, G.729, G729a, G.729b, G.729ab, and iLBC. These phones also support uncompressed wideband (16 bits, 16 kHz) audio.

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

The following sections describe the phone components.

Cisco Unified IP Phone 7975G Buttons and Hardware

The following figure identifies the important parts of the phone. See Buttons and Hardware Identification, on page 4 for the description of the numbered items.

Cisco Unified IP Phone 7970G and 7971G-GE Buttons and Hardware

The following figure identifies the important parts of the phone. See Buttons and Hardware Identification, on page 4 for the description of the numbered items.
Cisco Unified IP Phone 7965G Buttons and Hardware

The following figure identifies the important parts of the phone. See Buttons and Hardware Identification, on page 4 for the description of the numbered items.

Cisco Unified IP Phone 7945G Buttons and Hardware

The following figure identifies the important parts of the phone. See Buttons and Hardware Identification, on page 4 for the description of the numbered items.
Buttons and Hardware Identification

The following table describes the buttons and hardware on the phones.

**Table 1: Phone Buttons and Hardware**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1    | Programmable buttons | Depending on configuration, programmable buttons provide access to:  
|      |              | • Phone lines (line buttons) and intercom lines  
|      |              | • Speed-dial numbers (speed-dial buttons), including the Busy Lamp Field (BLF) speed-dial feature  
|      |              | • Web-based services (for example, a Personal Address Book button)  
|      |              | • Call features (for example, a Privacy, Hold, or Transfer button)  
|      | Buttons illuminate to indicate status:  
|      | • 🟢 Green, steady: Active call or two-way intercom call  
|      | • 🟢 Green, flashing: Held call  
|      | • 🟤 Amber, steady: Privacy in use, one-way intercom call, Do Not Disturb (DND) active, or logged into Hunt Group  
|      | • 🟤 Amber, flashing: Incoming call or reverting call  
|      | • 🔴 Red, steady: Remote line in use (shared line, BLF status or active Mobile Connect call)  
<p>| 2    | Footstand button | Enables you to adjust the angle of the phone base. |</p>
<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| 3    | **Display button**  
**Cisco Unified IP Phones 7970G, 7971G-GE, and 7975G**  
- Awakens the phone screen from sleep mode or disables the touchscreen feature for cleaning.  
- ![No color: Ready for input](image) No color: Ready for input  
- ![Green flashing: Disabled](image) Green flashing: Disabled  
- ![Green steady: Sleep mode](image) Green steady: Sleep mode  
**Cisco Unified IP Phones 7945G and 7965G**  
- Awakens the phone screen from sleep mode.  
- ![No color: Ready for input](image) No color: Ready for input  
- ![Green steady: Sleep mode](image) Green steady: Sleep mode |
| 4    | **Messages button**  
Autodials your voice message service (varies by service). |
| 5    | **Directories button**  
Opens/closes the Directories menu. Use the button to access call logs and directories. |
| 6    | **Help button**  
Activates the Help menu. |
| 7    | **Settings button**  
Opens/closes the Settings menu. Use the button to change phone screen and ring settings. |
| 8    | **Services button**  
Opens/closes the Services menu. |
| 9    | **Volume button**  
Controls the handset, headset, and speakerphone volume (off-hook) and the ringer volume (on-hook). |
| 10   | **Speaker button**  
Selects the speakerphone as the default audio path and initiates a new call, picks up an incoming call, or ends a call. During a call, the button is lit green.  
The speakerphone audio path does not change until you select a new default audiopath (for example, by picking up the handset).  
If external speakers are connected, the Speakerphone button uses these speakers as the default audio path. |
| 11   | **Mute button**  
Toggles the microphone on or off. When the microphone is muted, the button is lit. |
### Network Protocols

Cisco Unified IP Phones support 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 Cisco Unified IP Phone 7975G, 7971G-GE, 7970G, 7965G, and 7945G supports.

**Table 2: Supported Network Protocols on the Cisco Unified IP Phone**

<table>
<thead>
<tr>
<th>Network protocol</th>
<th>Purpose</th>
<th>Usage notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bootstrap Protocol (BootP)</td>
<td>BootP enables a network device such as the Cisco Unified IP Phone to</td>
<td>If you are using BootP to assign IP addresses to the Cisco Unified IP Phone, the BOOTP Server option shows “Yes” in the network configuration settings on the phone.</td>
</tr>
<tr>
<td></td>
<td>discover certain startup information, such as its IP address.</td>
<td></td>
</tr>
<tr>
<td>Network protocol</td>
<td>Purpose</td>
<td>Usage notes</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Cisco Discovery Protocol (CDP)</td>
<td>CDP is a device-discovery protocol that runs on all Cisco-manufactured equipment. By using CDP, a device can advertise its existence to other devices and receive information about other devices in the network.</td>
<td>The Cisco Unified IP 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.</td>
</tr>
<tr>
<td>Cisco Peer-to-Peer Distribution Protocol (CPPDP)</td>
<td>CPPDP is a Cisco proprietary protocol that forms a peer-to-peer hierarchy of devices. CPPDP also copies firmware or other files from peer devices to neighboring devices.</td>
<td>The Peer Firmware Sharing feature uses CPPDP.</td>
</tr>
<tr>
<td>Dynamic Host Configuration Protocol (DHCP)</td>
<td>DHCP dynamically allocates and assigns an IP address to network devices. DHCP enables you to connect an IP phone into the network and have the phone become operational without the need to assign an IP address manually or to configure additional network parameters.</td>
<td>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. Cisco recommends 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 “Dynamic Host Configuration Protocol” and “Cisco TFTP” chapters in the Cisco Unified Communications Manager System Guide.</td>
</tr>
<tr>
<td>Hypertext Transfer Protocol (HTTP)</td>
<td>HTTP is the standard way of transferring information and moving documents across the Internet and the web.</td>
<td>Cisco Unified IP Phones use HTTP for XML services and for troubleshooting purposes. The phones use HTTP to download configuration files and firmware loads. If the HTTP download fails, the phone uses TFTP to transfer the files. Cisco Unified IP Phones do not support the use of IPv6 addresses in the URL. You cannot use a literal IPv6 address in the URL or a hostname that maps to an IPv6 address.</td>
</tr>
<tr>
<td>Hypertext Transfer Protocol Secure (HTTPS)</td>
<td>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.</td>
<td>Web applications with both HTTP and HTTPS support have two URLs configured. For a Cisco Unified IP Phone that supports HTTPS, choose the HTTPS URL from the two URLs.</td>
</tr>
<tr>
<td>Network protocol</td>
<td>Purpose</td>
<td>Usage notes</td>
</tr>
<tr>
<td>--------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IEEE 802.1X</td>
<td>The IEEE 802.1X standard defines a client-server-based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. Until the client authenticates, 802.1X access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the client connects. After authentication is successful, normal traffic can pass through the port.</td>
<td>The Cisco Unified IP Phone implements the IEEE 802.1X standard by supporting the following authentication methods: EAP-FAST, EAP-TLS, and EAP-MD5. When 802.1X authentication is enabled on the phone, you should disable the PC port and voice VLAN. See <a href="#">802.1X Authentication</a> on page 21 for additional information.</td>
</tr>
<tr>
<td>Internet Protocol (IP)</td>
<td>IP is a messaging protocol that addresses and sends packets across the network.</td>
<td>To communicate by using IP, network devices must have an assigned IP address, subnet, and gateway. IP addresses, subnets, and gateways identifications are automatically assigned if you use the Cisco Unified IP Phone with Dynamic Host Configuration Protocol (DHCP). If you do not use DHCP, you must manually assign these properties to each phone locally. The Cisco Unified IP Phone supports concurrent IPv4 and IPv6 addresses. Configure the IP addressing mode (IPv4 only, IPv6 only, or both IPv4 and IPv6) in Cisco Unified Communications Manager Administration. For more information, see the &quot;Internet Protocol Version 6 (IPv6)&quot; chapter in the <em>Cisco Unified Communications Manager Features and Services Guide</em>.</td>
</tr>
<tr>
<td>Link Layer Discovery Protocol (LLDP)</td>
<td>LLDP is a standardized network discovery protocol (similar to CDP) that some Cisco and third-party devices support.</td>
<td>The Cisco Unified IP Phone supports LLDP on the PC port.</td>
</tr>
<tr>
<td>Network protocol</td>
<td>Purpose</td>
<td>Usage notes</td>
</tr>
<tr>
<td>-------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Link Layer Discovery Protocol-Media Endpoint Devices</td>
<td>LLDP-MED is an extension of the LLDP standard developed for voice</td>
<td>The Cisco Unified IP Phone supports LLDP-MED on the SW port to communicate information such as:</td>
</tr>
</tbody>
</table>
| (LLDP-MED)                                            | products.                                                             |   • Voice VLAN configuration  
   • Device discovery  
   • Power management  
   • Inventory management                                                                                                                                  |
|                                                        |                                                                        | For more information about LLDP-MED support, see the LLDP-MED and Cisco Discovery Protocol white paper:                                                                                                      |
| Real-Time Control Protocol (RTCP)                     | RTCP works with Real-Time Transport Protocol (RTP) to provide QoS     | RTCP is disabled by default, but you can enable it on a per-phone basis in Cisco Unified Communications Manager Administration. For more information, see Network Configuration Menu, on page 103.                           |
|                                                        | data (such as jitter, latency, and round trip delay) on RTP streams.  |                                                                                                                                                                                                          |
| Real-Time Transport Protocol (RTP)                    | RTP is a standard protocol for transport of real-time data, such as  | Cisco Unified IP Phones use the RTP protocol to send and receive real-time voice traffic from other phones and gateways.                                                                                     |
|                                                        | interactive voice and video, over data networks.                      |                                                                                                                                                                                                          |
| Session Initiation Protocol (SIP)                     | SIP is the Internet Engineering Task Force (IETF) standard for        | Like other VoIP protocols, SIP addresses 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. |
|                                                        | multimedia conferencing over IP. SIP is an ASCII-based application-    | You can configure the Cisco Unified IP Phone to use either SIP or Skinny Client Control Protocol (SCCP). Cisco Unified IP Phones do not support the SIP protocol when the phones operate in IPv6 address mode. |
|                                                        | layer control protocol (defined in RFC 3261) that can establish,     |                                                                                                                                                                                                          |
|                                                        | maintain, and terminate calls between two or more endpoints.         |                                                                                                                                                                                                          |

## Network Protocols

<table>
<thead>
<tr>
<th>Network protocol</th>
<th>Purpose</th>
<th>Usage notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skinny Client Control Protocol (SCCP)</td>
<td>SCCP includes a messaging set that allows communications between call control servers and endpoint clients such as IP Phones. SCCP is proprietary to Cisco Systems.</td>
<td>Cisco Unified IP Phones use SCCP for call control. You can configure the Cisco Unified IP Phone to use either SCCP or Session Initiation Protocol (SIP).</td>
</tr>
<tr>
<td>Session Description Protocol (SDP)</td>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td>Transmission Control Protocol (TCP)</td>
<td>TCP is a connection-oriented transport protocol.</td>
<td>Cisco Unified IP Phones use TCP to connect to Cisco Unified Communications Manager and to access XML services.</td>
</tr>
<tr>
<td>Transport Layer Security (TLS)</td>
<td>TLS is a standard protocol for securing and authenticating communications.</td>
<td>When security is implemented, Cisco Unified IP Phones use the TLS protocol for secure registration with Cisco Unified Communications Manager. For more information, see the Cisco Unified Communications Manager Security Guide.</td>
</tr>
<tr>
<td>Trivial File Transfer Protocol (TFTP)</td>
<td>TFTP allows you to transfer files over the network. On the Cisco Unified IP Phone, TFTP enables you to obtain a configuration file that is specific to the phone type.</td>
<td>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 that the DHCP server specifies, you must manually assign TFTP server from the Network Configuration menu on the phone. For more information, see the &quot;Cisco TFTP&quot; chapter in the Cisco Unified Communications Manager System Guide.</td>
</tr>
<tr>
<td>User Datagram Protocol (UDP)</td>
<td>UDP is a connectionless messaging protocol for delivery of data packets.</td>
<td>Cisco Unified IP Phones transmit and receive RTP streams, which utilize UDP.</td>
</tr>
</tbody>
</table>
IPv6 Support on Cisco Unified IP Phones

The Cisco Unified IP Phones use the Internet Protocol to provide voice communication over the network. Because Internet Protocol version 4 (IPv4) uses a 32-bit address, it cannot meet the increased demands for unique IP addresses for all devices that connect to the internet. Therefore, Internet Protocol version 6 (IPv6) is an updated version of the current Internet Protocol. IPv6 uses a 128-bit address and provides end-to-end security capabilities, enhanced Quality of Service (QoS), and increased number of available IP addresses.

The Cisco Unified IP Phone supports IPv4-only addressing mode, IPv6-only addressing mode, as well as an IPv4/IPv6 dual stack addressing mode. In IPv4, you can enter each octet of the IP address on the phone in dotted decimal notation; for example, 192.240.22.5. In IPv6, you can enter each octet of the IP address in hexadecimal notation with each octet separated by a colon; for example, 2005:db8:0:1:ef8:9876:ba72:dc9a. The phone truncates and removes leading zeros when it displays the IPv6 address.

Cisco Unified IP Phones support both IPv4 and IPv6 addresses transparently, so users can handle all calls on the phone to which they are accustomed. Cisco Unified IP Phones with the Skinny Call Control Protocol (SCCP) support IPv6. Cisco Unified IP Phones with SIP do not support IPv6.

Cisco Unified IP Phones do not support URLs with IPv6 addresses in the URL. This affects all IP Phone Service URLs, such as services, directories, messages, help, and any restricted web services that require the phone to use the HTTP protocol to validate credentials with the Authentication URL. If you configure Cisco Unified IP Phone services for Cisco Unified IP Phones, you must configure the phone and the servers that support the phone service with IPv4 addresses.

If you configure IPv6 Only as the IP Addressing Mode for phones that are running SIP, the Cisco TFTP service overrides the IP Addressing Mode configuration and uses IPv4 Only in the configuration file.


Cisco Unified IP Phone 7975G, 7971G-GE, 7970G, 7965G, and 7945G Supported Features

The Cisco Unified IP Phone functions much like a digital business phone and allows you to place and receive telephone calls. In addition to traditional telephony features, the Cisco Unified IP Phone includes features that enable you to administer and monitor the phone as a network device.

This section includes the following topics:

Feature Overview

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

As with other network devices, you must configure Cisco Unified IP Phones to prepare them to access Cisco Unified Communications Manager and the rest of the IP network. By using DHCP, you have fewer
settings to configure on a phone, but if your network requires it, you can manually configure an IP address, TFTP server, subnet information, and other values.

The Cisco Unified IP Phone interacts with other services and devices on your IP network to provide enhanced functionality. For example, you can integrate the Cisco Unified IP Phones 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. You can also use XML to enable users to access information such as weather, stocks, quote of the day, and other web-based information.

Finally, because the Cisco Unified IP Phone is a network device, you can obtain detailed status information from it directly. This information can assist you with troubleshooting any problems that users encounter when they use their IP phones.

Related Topics

- Cisco Unified IP Phone Settings, on page 61
- Features, Templates, Services, and Users, on page 123
- Services Setup, on page 155
- Model Information, Status, and Statistics, on page 177
- Troubleshooting and Maintenance, on page 217
- Corporate Directory Setup, on page 151

Telephony Feature Administration

You can modify certain settings for the Cisco Unified IP Phone from the Cisco Unified Communications Manager Administration application. Use this graphical user interface 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. See the Cisco Unified Communications Manager Administration Guide for additional information.

For more information about the Cisco Unified Communications Manager Administration application, refer to Cisco Unified Communications Manager documentation, including the Cisco Unified Communications Manager System Guide. You can also use the context-sensitive help that is available within the application for guidance.

You can access the Cisco Unified Communications Manager documentation suite at this location:

You can access the complete Cisco Business Edition 5000 documentation suite at this location:

Related Topics

- Telephony Features Available for Cisco Unified IP Phone, on page 124

Cisco Unified IP Phone Network Parameters

You can configure parameters such as DHCP, TFTP, and IP settings on the phone itself. You can also obtain statistics about a current call or firmware versions on the phone.

Related Topics

- Cisco Unified IP Phone Settings, on page 61
Information for End Users

If you are a system administrator, you are likely the primary source of information for Cisco Unified IP Phone users in your network or company. To ensure that you distribute the most current feature and procedural information, familiarize yourself with Cisco Unified IP Phone documentation. Make sure to visit the Cisco Unified IP Phone web site:


From this site, you can access various user guides.

In addition to providing users with documentation, it is important to inform them about available Cisco Unified IP Phone features, including features that are specific to your company or network, and about how to access and customize those features, if appropriate.

Related Topics

Internal Support Web Site, on page 243

Cisco Unified IP Phone Security Features

Implementation of security in the Cisco Unified Communications Manager system prevents identity theft of the phone and Cisco Unified Communications Manager server, prevents data tampering, and prevents call signaling and media stream tampering.

To alleviate these threats, the Cisco Unified IP telephony network establishes and maintains authenticated and encrypted communication streams between a phone and the server, digitally signs files before they are transferred to a phone, and encrypts media streams and call signaling between Cisco Unified IP phones.

The Cisco Unified IP Phone 7975G, 7971G-GE, 7970G, 7965G, and 7945G uses the Phone Security Profile, which defines whether the device is nonsecure, authenticated, or encrypted. For information on application of the security profile to the phone, see the Cisco Unified Communications Manager Security Guide.

If you configure security-related settings in Cisco Unified Communications Manager Administration, the phone configuration file will contain sensitive information. To ensure the privacy of a configuration file, you must configure it for encryption. For detailed information, see the “Configuring Encrypted Phone Configuration Files” chapter in the Cisco Unified Communications Manager Security Guide.

The following table shows where you can find additional information about security in this and other documents.

<table>
<thead>
<tr>
<th>Topic</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detailed explanation of security; includes setup, configuration, and troubleshooting information for Cisco Unified Communications Manager and Cisco Unified IP Phones</td>
<td>See the Troubleshooting Guide for Cisco Unified Communications Manager.</td>
</tr>
<tr>
<td>Security features that the Cisco Unified IP Phone supports</td>
<td>See Supported Security Features, on page 15.</td>
</tr>
<tr>
<td>Topic</td>
<td>Reference</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Viewing a security profile name</td>
<td>See Security Profiles, on page 17.</td>
</tr>
<tr>
<td>Identification of phone calls for which security is implemented</td>
<td>See Authenticated, Encrypted, and Protected Phone Calls, on page 18.</td>
</tr>
<tr>
<td>TLS connection</td>
<td>See Network Protocols, on page 6.</td>
</tr>
<tr>
<td></td>
<td>See Phone Configuration Files, on page 34.</td>
</tr>
<tr>
<td>Security and the phone startup process</td>
<td>See Phone Startup Process, on page 36.</td>
</tr>
<tr>
<td>Security and phone configuration files</td>
<td>See Phone Configuration Files, on page 34.</td>
</tr>
<tr>
<td>Changes to the TFTP Server 1 or TFTP Server 2 option on the phone</td>
<td>See Network Configuration Menu, on page 66.</td>
</tr>
<tr>
<td>Security icons in the Unified CM 1 through Unified CM 5 options in the Device Configuration Menu on the phone</td>
<td>See Unified CM Configuration Menu, on page 85.</td>
</tr>
<tr>
<td>Security Configuration menu items that you access from the Device Configuration menu on the phone</td>
<td>See Security Configuration Menu, on page 101.</td>
</tr>
<tr>
<td>Security Configuration menu items that you access from the Settings menu on the phone</td>
<td>See Security Configuration Menu, on page 109.</td>
</tr>
<tr>
<td>Unlock of the CTL (Certificate Trust List) and ITL (Identity Trust List) files</td>
<td>See Unlock CTL and ITL Files, on page 113.</td>
</tr>
<tr>
<td>Disabling access to web pages for a phone</td>
<td>See Unlock CTL and ITL Files, on page 113.</td>
</tr>
<tr>
<td>Deletion of the CTL file from the phone</td>
<td>See Control Web Page Access, on page 201.</td>
</tr>
<tr>
<td>Phone reset or restoration</td>
<td>See Cisco Unified IP Phone Reset or Restore, on page 236.</td>
</tr>
<tr>
<td>Extension Mobility HTTPS Support</td>
<td>See Network Protocols, on page 6.</td>
</tr>
<tr>
<td>802.1X Authentication for Cisco Unified IP Phones</td>
<td>See these sections:</td>
</tr>
<tr>
<td></td>
<td>• 802.1X Authentication, on page 21</td>
</tr>
<tr>
<td></td>
<td>• 802.1X Authentication and Status Menus, on page 116</td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified IP Phone Security Problems, on page 224</td>
</tr>
</tbody>
</table>
Supported Security Features

The following table provides an overview of the security features that the Cisco Unified IP Phone 7975G, 7971G-GE, 7970G, 7965G, and 7945G supports. For more information about these features and about Cisco Unified Communications Manager and Cisco Unified IP Phone security, see the Cisco Unified Communications Manager Security Guide.

For information about current security settings on a phone, look at the Security Configuration menus on the phone (choose Settings > Security Configuration and choose Settings > Device Configuration > Security Configuration).

Note

Most security features are available only if a CTL is installed on the phone. For more information about the CTL, see the “Configuring the Cisco CTL Client” chapter in the Cisco Unified Communications Manager Security Guide.

Table 4: Overview of security features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image authentication</td>
<td>Signed binary files (with the extension .sbn) prevent tampering with the firmware image before it loads on a phone. Tampering with the image causes a phone to fail the authentication process and reject the new image.</td>
</tr>
<tr>
<td>Customer-site certificate</td>
<td>Each Cisco Unified IP Phone requires a unique certificate for device authentication. Phones include a manufacturing installed certificate (MIC),</td>
</tr>
<tr>
<td>installation</td>
<td>but for additional security, you can specify in Cisco Unified Communications Manager Administration that a certificate be installed by using the CAPF (Certificate Authority Proxy Function). Alternatively, you can install a Locally Significant Certificate (LSC) from the Security Configuration menu on the phone.</td>
</tr>
<tr>
<td>Device authentication</td>
<td>Occurs between the Cisco Unified Communications Manager server and the phone when each entity accepts the certificate of the other entity. Determines whether a secure connection between the phone and a Cisco Unified Communications Manager should occur, and, if necessary, creates a secure signaling path between the entities that use TLS protocol. Cisco Unified Communications Manager does not register phones unless it can authenticate them.</td>
</tr>
<tr>
<td>File authentication</td>
<td>Validates digitally signed files that the phone downloads. The phone validates the signature to make sure that file tampering did not occur after file creation. Files that fail authentication are not written to Flash memory on the phone. The phone rejects such files without further processing.</td>
</tr>
<tr>
<td>Signaling authentication</td>
<td>Uses the TLS protocol to validate that no tampering has occurred to signaling packets during transmission.</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Manufacturing installed certificate</td>
<td>Each Cisco Unified IP Phone contains a unique manufacturing installed certificate (MIC), which is used for device authentication. The MIC is a permanent unique proof of identity for the phone, and allows Cisco Unified Communications Manager to authenticate the phone.</td>
</tr>
<tr>
<td>Secure SRST reference</td>
<td>After you configure an SRST reference for security and then reset the dependent devices in Cisco Unified Communications Manager Administration, the TFTP server adds the SRST certificate to the phone cnf.xml file and sends the file to the phone. A secure phone then uses a TLS connection to interact with the SRST-enabled router.</td>
</tr>
<tr>
<td>Media encryption</td>
<td>Uses Secure Real-time Transport Protocol (SRTP) to ensure that the media streams between supported devices prove secure and that only the intended device receives and reads the data. Includes creation of a media master key pair for the devices, delivery of the keys to the devices, and securing the key delivery while the keys are in transport.</td>
</tr>
<tr>
<td>Signaling encryption</td>
<td>Ensures that all SCCP and SIP signaling messages that are sent between the device and the Cisco Unified Communications Manager server are encrypted.</td>
</tr>
<tr>
<td>CAPF (Certificate Authority Proxy Function)</td>
<td>Implements parts of the certificate generation procedure that are too processing-intensive for the phone, and interacts with the phone for key generation and certificate installation. The CAPF can be configured to request certificates from customer-specified certificate authorities on behalf of the phone, or it can be configured to generate certificates locally.</td>
</tr>
<tr>
<td>Security profiles</td>
<td>Defines whether the phone is nonsecure, authenticated, encrypted, or protected.</td>
</tr>
<tr>
<td>Encrypted configuration files</td>
<td>Ensures the privacy of phone configuration files.</td>
</tr>
<tr>
<td>Optional disabling of the web server function for a phone</td>
<td>Prevents access to a phone web page, which displays a variety of operational statistics for the phone.</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Additional security options, which you control from Cisco Unified Communications Manager Administration:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Disabling PC port</td>
</tr>
<tr>
<td></td>
<td>• Disabling Gratuitous ARP (GARP)</td>
</tr>
<tr>
<td></td>
<td>• Disabling PC Voice VLAN access</td>
</tr>
<tr>
<td></td>
<td>• Disabling access to the Setting menus, or providing restricted access that allows access to the User Preferences menu and saving volume changes only</td>
</tr>
<tr>
<td></td>
<td>• Disabling access to web pages for a phone</td>
</tr>
<tr>
<td>Note</td>
<td>View current settings for the PC Port Disabled, GARP Enabled, and Voice VLAN enabled options by looking at the phone Security Configuration menu.</td>
</tr>
<tr>
<td>802.1X Authentication</td>
<td>The Cisco Unified IP Phone can use 802.1X authentication to request and gain access to the network.</td>
</tr>
</tbody>
</table>

**Related Topics**

- Security Profiles, on page 17
- Authenticated, Encrypted, and Protected Phone Calls, on page 18
- Secure Conference Call Identification, on page 18
- Device Configuration Menu, on page 85
- 802.1X Authentication, on page 21
- Cisco Unified IP Phone Security, on page 58
- Cisco Unified IP Phone Settings, on page 61
- Security Restrictions, on page 23

**Security Profiles**

Cisco Unified IP Phones that support Cisco Unified Communications Manager release 7.0 or later use a security profile, which defines whether the phone is nonsecure, authenticated, or encrypted. For information about security profile configuration and profile application to the phone, see the *Cisco Unified Communications Manager Security Guide*.

To view the security mode that is set for the phone, view the Security Mode setting in the Security Configuration menu.

**Related Topics**

- Authenticated, Encrypted, and Protected Phone Calls, on page 18
- Device Configuration Menu, on page 85
- Security Configuration Menu, on page 101
- Security Restrictions, on page 23
Authenticated, Encrypted, and Protected Phone Calls

When security is implemented for a phone, you can identify authenticated or encrypted phone calls by icons on the phone screen. You can also determine whether the connected phone is secure and protected if a security tone plays at the beginning of the call.

In an authenticated call, all devices that participate in the establishment of the call are trusted devices that Cisco Unified Communications Manager authenticates. When a call in progress is authenticated, the call progress icon to the right of the call duration timer in the phone screen changes to this icon:

In an encrypted call, all devices that participate in the establishment of the call are trusted devices that Cisco Unified Communications Manager authenticates. In addition, call signaling and media streams are encrypted. An encrypted call offers a high level of security and provides integrity and privacy to the call. When a call in progress is encrypted, the call progress icon to the right of the call duration timer in the phone screen changes to this icon:

Note

If the call routes through non-IP call legs, for example, PSTN (public switched telephone network), the call may be nonsecure even though it is encrypted within the IP network and has a lock icon associated with it.

In a protected call, a security tone plays at the beginning of a call to indicate that the other connected phone is also receiving and transmitting encrypted audio and video (if video is involved). If your call connects to a non-protected phone, the security tone does not play.

Note

Protected calling is supported for connections between two phones only. Some features, such as conference calling, shared lines, Extension Mobility, and Join Across Lines are not available when protected calling is configured. Protected calls are not authenticated.

Related Topics

- Cisco Unified IP Phone Security Features, on page 13
- Security Profiles, on page 17
- Security Restrictions, on page 23

Secure Conference Call Identification

You can initiate a secure conference call and monitor the security level of participants. Establishment of a secure conference call follows this process:

1. A user initiates the conference from a secure phone (encrypted or authenticated security mode).
2. Cisco Unified Communications Manager assigns a secure conference bridge to the call.
3. As participants are added, Cisco Unified Communications Manager verifies the security mode of each phone (encrypted or authenticated) and maintains the secure level for the conference.
4 The phone displays the security level of the conference call. A secure conference displays ☑ (encrypted) or ☑ (authenticated) icon to the right of “Conference” on the phone screen. If ☑ icon displays, the conference is not secure.

---

**Note**

Certain interactions, restrictions, and limitations affect the security level of the conference call. These interactions depend on the security mode of the participant phones and the availability of secure conference bridges. See Call Security Interactions and Restrictions, on page 19 for information about these interactions.

---

**Protected Call Identification**

A protected call is established when a user phone and the phone on the other end are configured for protected calling. The other phone can be in the same Cisco IP network, or on a network outside the IP network. Protected calls can only be made between two phones. Conference calls and other multiple-line calls are not supported.

Establishment of a protected call follows this process:

1. A user initiates the call from a protected phone (protected security mode).
2. The phone displays the ☑ icon (encrypted) on the phone screen. This icon indicates that the phone is configured for secure (encrypted) calls, but this does not mean that the other connected phone is also protected.
3. A security tone plays if the call connects to another protected phone; the tone indicates that both ends of the conversation are encrypted and protected. If the call is connected to a nonprotected phone, the secure tone does not play.

---

**Call Security Interactions and Restrictions**

Cisco Unified Communications Manager checks the phone security status when conferences are established and changes the security indication for the conference or blocks the completion of the call to maintain integrity and also security in the system. The following table provides information about changes to call security levels when the Barge feature is used.

**Table 5: Call Security Interactions When using Barge**

<table>
<thead>
<tr>
<th>Initiator phone security level</th>
<th>Call security level</th>
<th>Results of action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nonsecure</td>
<td>Encrypted call</td>
<td>Call barged and identified as nonsecure call</td>
</tr>
<tr>
<td>Secure (encrypted)</td>
<td>Authenticated call</td>
<td>Call barged and identified as authenticated call</td>
</tr>
<tr>
<td>Initiator phone security level</td>
<td>Call security level</td>
<td>Results of action</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Secure (authenticated)</td>
<td>Encrypted call</td>
<td>Call barged and identified as authenticated call</td>
</tr>
<tr>
<td>Nonsecure</td>
<td>Authenticated call</td>
<td>Call barged and identified as nonsecure call</td>
</tr>
</tbody>
</table>

The following table provides information about changes to conference security levels, which depend on the initiator phone security level, the security levels of participants, and the availability of secure conference bridges.

**Table 6: Security Restrictions with Conference Calls**

<table>
<thead>
<tr>
<th>Initiator phone security level</th>
<th>Feature used</th>
<th>Security level of participants</th>
<th>Results of action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nonsecure</td>
<td>Conference</td>
<td>Encrypted or authenticated</td>
<td>Nonsecure conference bridge Nonsecure conference</td>
</tr>
<tr>
<td>Secure (encrypted or authenticated)</td>
<td>Conference</td>
<td>At least one member is nonsecure.</td>
<td>Secure conference bridge Nonsecure conference</td>
</tr>
<tr>
<td>Secure (encrypted)</td>
<td>Conference</td>
<td>All participants are encrypted</td>
<td>Secure conference bridge Secure encrypted level conference</td>
</tr>
<tr>
<td>Secure (authenticated)</td>
<td>Conference</td>
<td>All participants are encrypted or authenticated.</td>
<td>Secure conference bridge Secure authenticated level conference</td>
</tr>
<tr>
<td>Nonsecure</td>
<td>Conference</td>
<td>Encrypted or authenticated</td>
<td>Only secure conference bridge is available and used Nonsecure conference</td>
</tr>
<tr>
<td>Secure (encrypted or authenticated)</td>
<td>Conference</td>
<td>Encrypted or authenticated</td>
<td>Only nonsecure conference bridge is available and used Nonsecure conference</td>
</tr>
<tr>
<td>Secure (encrypted or authenticated)</td>
<td>Conference</td>
<td>Secure or encrypted</td>
<td>Conference remains secure When one participant tries to Hold the call with Music on Hold (MOH), the MOH does not play.</td>
</tr>
<tr>
<td>Initiator phone security level</td>
<td>Feature used</td>
<td>Security level of participants</td>
<td>Results of action</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------</td>
<td>--------------------------------</td>
<td>-------------------</td>
</tr>
</tbody>
</table>
| Secure (encrypted)            | Join        | Encrypted or authenticated     | Secure conference bridge  
Conference remains secure (encrypted or authenticated) |
| Nonsecure                    | cBarge      | All participants are encrypted | Secure conference bridge  
Conference changes to nonsecure |
| Nonsecure                    | Meet-Me     | Minimum security level is encrypted | Initiator receives message  
Does not meet Security Level, call rejected. |
| Secure (encrypted)           | Meet-Me     | Minimum security level is authenticated | Secure conference bridge  
Conference accepts encrypted and authenticated calls |
| Secure (encrypted)           | Meet-Me     | Minimum security level is nonsecure | Only secure conference bridge available and used  
Conference accepts all calls |

### 802.1X Authentication

These sections provide information about 802.1X support on the Cisco Unified IP Phones:

#### Overview

Cisco Unified IP Phones and Cisco Catalyst switches traditionally use Cisco Discovery Protocol (CDP) to identify each other and determine parameters such as VLAN allocation and inline power requirements. CDP does not identify locally attached workstations. Cisco Unified IP Phones provide an EAPOL pass-through mechanism. This mechanism allows a workstation attached to the Cisco Unified 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 Unified 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.

Cisco Unified IP Phones also 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, EAP-TLS, and EAP-MD5 options for network authentication.
Required Network Components

Support for 802.1X authentication on Cisco Unified IP Phones requires several components, including:

• Cisco Unified IP Phone: The phone acts as the 802.1X supplicant, which initiates the request to access the network.

• 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.

• Cisco Catalyst Switch (or other third-party switch): The switch must support 802.1X, so it can act 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.

Best-Practice Requirements and Recommendations

• Enable 802.1X Authentication: If you want to use the 802.1X standard to authenticate Cisco Unified IP Phones, make sure that you have properly configured the other components before you enable the standard on the phone.


• Configure PC Port: The 802.1X standard does not take into account the use of VLANs and thus recommends that only a single device be authenticated to a specific switch port. However, some switches (such as Cisco Catalyst switches) support multidomain authentication. The switch configuration determines whether you can connect a PC to the phone PC port.

   • Enabled: If you use a switch that supports multidomain authentication, you can enable the PC port and connect a PC to it. In this case, Cisco Unified IP Phones support proxy EAPOL-Logoff to monitor the authentication exchanges between the switch and the attached PC. For more information about IEEE 802.1X support on the Cisco Catalyst switches, see the Cisco Catalyst switch configuration guides at:


   • Disabled: 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 will deny network access to the phone and the PC.

• Configure Voice VLAN: Because the 802.1X standard does not account for VLANs, you should configure this setting according to the switch support.

   • Enabled: If you use 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.

• Enter MD5 Shared Secret: If you disable 802.1X authentication or perform a factory reset on the phone, the previously configured MD5 shared secret is deleted.
Security Restrictions

A user cannot barge into an encrypted call if the phone that is used to barge is not configured for encryption. When barge fails in this case, a reorder (fast busy) tone plays on the phone of the barge initiator.

If the initiator phone is configured for encryption, the barge initiator can barge into an authenticated or nonsecure call from the encrypted phone. After the barge occurs, Cisco Unified Communications Manager classifies the call as nonsecure.

If the initiator phone is configured for encryption, the barge initiator can barge into an encrypted call, and the phone indicates that the call is encrypted.

A user can barge into an authenticated call, even if the phone that is used to barge is nonsecure. The authentication icon continues to appear on the authenticated devices in the call, even if the initiator phone does not support security.

Phone Power Consumption

The Cisco Unified IP Phone 7900 Series supports Cisco EnergyWise. EnergyWise is also known as Power Save Plus. When your network contains an EnergyWise controller, you can configure these phones to sleep (power down) and wake (power up) on a schedule to reduce your power consumption. The phone should be powered by the Power Over Ethernet (PoE) port of the switch instead of the power adapter.

You set up each phone to enable or disable the EnergyWise settings. You can also configure EnergyWise parameters on the enterprise and common phone configuration. If EnergyWise is enabled, you configure a sleep and wake time, as well as other parameters. These parameters are sent to the phone as part of the phone configuration XML file.

The switch administrator can wake the phone up before the scheduled time. For more information on powering up the phones from the switch, see the switch documentation.

Cisco Unified IP Phone Deployment

Upon deployment of a new IP telephony system, system administrators and network administrators must complete several initial configuration tasks to prepare the network for IP telephony service. For information and a checklist for setup and configuration of a Cisco Unified IP telephony network, see the "System Configuration Overview" chapter in the Cisco Unified Communications Manager System Guide.

After you have set up the IP telephony system and configured system-wide features in Cisco Unified Communications Manager, you can add IP phones to the system.

The following topics provide an overview of procedures for adding Cisco Unified IP Phones to your network:
Cisco Unified IP Phone Setup in Cisco Unified Communications Manager

To add phones to the Cisco Unified Communications Manager database, you can use:

• Autoregistration
• Cisco Unified Communications Manager Administration
• Bulk Administration Tool (BAT)
• BAT and the Tool for Auto-Registered Phones Support (TAPS)

For general information about phone configuration in Cisco Unified Communications Manager, see the "Cisco Unified IP Phones" chapter in the Cisco Unified Communications Manager System Guide.

Related Topics
Cisco Unified Communications Manager Phone Addition Methods, on page 37

Set Up Cisco Unified IP Phone 7975G, 7971G-GE, 7970G, 7965G, and 7945G in Cisco Unified Communications Manager Administration

The following steps provide an overview and checklist of configuration tasks for the Cisco Unified IP Phone 7975G, 7971G-GE, 7970G, 7965G, and 7945G in Cisco Unified Communications Manager Administration. The steps present a suggested order to guide you through the phone configuration process. Some tasks are optional, depending on your system and user needs. For detailed procedures and information, see the sources in the steps.

Procedure

Step 1  Gather the following information about the phone:
   a) Phone Model
   b) MAC address
   c) Physical location of the phone
   d) Name or user ID of phone user
   e) Device pool
   f) Partition, calling search space, and location information
   g) Number of lines and associated directory numbers (DNs) to assign to the phone
   h) Cisco Unified Communications Manager user to associate with the phone
   i) Phone usage information that affects phone button template, softkey template, phone features, IP Phone services, or phone applications
      Provides list of configuration requirements for phone setup.
      Identifies preliminary configuration that you need to perform before you configure individual phones, such as phone button templates or softkey templates.

Step 2  Customize phone button templates (if required).
Changes the number of line buttons, speed-dial buttons, Service URL buttons, or adds a Privacy button to meet user needs.

You must specify a service URL with an IPv4 address.

See Cisco Unified Communications Manager Administration Guide, "Phone Button Template Configuration" chapter, and Phone Button Templates, on page 152.

**Step 3**  Add and configure the phone by completing the required fields in the Phone Configuration window. Required fields are indicated by an asterisk (*) next to the field name; for example, MAC address and device pool.

Adds the device with its default settings to the Cisco Unified Communications Manager database.

See the Cisco Unified Communications Manager Administration Guide, "Cisco Unified IP Phone Configuration" chapter. For information about Product Specific Configuration fields, refer to “?” button Help in the Phone Configuration window.

**Step 4**  Add and configure directory numbers (lines) on the phone by completing the required fields in the Directory Number Configuration window. Required fields are indicated by an asterisk (*) next to the field name; for example, directory number and presence group.

Adds primary and secondary directory numbers and features associated with directory numbers to the phone.

See the Cisco Unified Communications Manager Administration Guide, "Directory Number Configuration" chapter, and Telephony Features Available for Cisco Unified IP Phone, on page 124.

**Step 5**  Customize softkey templates.

Adds, deletes, or changes order of softkey features that display on the user phone to meet feature usage needs.

See the Cisco Unified Communications Manager Administration Guide, "Softkey Template Configuration" chapter, and Softkey Templates, on page 155.

**Step 6**  Configure speed-dial buttons and assign speed-dial numbers (optional). Add speed-dial buttons and numbers.

*Note*  Users can change speed-dial settings on their phones by using the Cisco Unified Communications Manager User Options web pages.

See the Cisco Unified Communications Manager Administration Guide, "Cisco Unified IP Phone Configuration" chapter.

**Step 7**  Configure Cisco Unified IP Phone services and assign services (optional). Provides IP Phone services.

*Note*  Users can add or change services on their phones by using the Cisco Unified Communications Manager User Options web pages.

*Note*  You must specify a service URL with an IPv4 address.

See the Cisco Unified Communications Manager Administration Guide "Cisco Unified IP Phone Services Configuration" chapter, and Services Setup, on page 155.

**Step 8**  Assign services to phone buttons (optional). Provides single-button access to an IP phone service or URL.

See the Cisco Unified Communications Manager Administration Guide, "Cisco Unified IP Phone Configuration" chapter.

**Step 9**  Add user information by configuring required fields. Required fields are indicated by an asterisk (*); for example, User ID and last name.

*Note*  Assign a password (for User Options web pages) and PIN (for Extension Mobility and Personal Directory).

Adds user information to the global directory for Cisco Unified Communications Manager.

See Cisco Unified Communications Manager Administration Guide, "End User Configuration" chapter and Cisco Unified Communications Manager User Addition, on page 156.
If your company uses a Lightweight Directory Access Protocol (LDAP) directory to store information on users, you can install and configure Cisco Unified Communications to use your existing LDAP directory, see Corporate Directory Setup, on page 151.

**Step 10**
Associate a user to a user group. Assigns users a common list of roles and permissions that apply to all users in a user group. Administrators can manage user groups, roles, and permissions to control the level of access (and, therefore, the level of security) for system users.

See the Cisco Unified Communications Manager Administration Guide:

- "End User Configuration" chapter
- "User Group Configuration" chapter

**Step 11**
Associate a user with a phone. Provides users with control over their phone so that they can forward calls or add speed-dial numbers or services.

Note Some phones, such as those in conference rooms, do not have an associated user.

See the Cisco Unified Communications Manager Administration Guide, "End User Configuration" chapter.

---

**Cisco Unified IP Phone Installation**

After you add the phones to the Cisco Unified Communications Manager database, you can complete the phone installation. You can install the phones at the desired locations, or you can give the phone users the information they need to perform the installation. The Cisco Unified IP Phone Installation Guide, which is available at [http://www.cisco.com/en/US/products/hw/phones/ps379/prod_installation_guides_list.html](http://www.cisco.com/en/US/products/hw/phones/ps379/prod_installation_guides_list.html), provides directions for connecting the phone foot stand, handset, cables, and other accessories.

**Note**
Upgrade the phone to the current firmware image before installation. For information about phone upgrades, see the Readme file for your phone model located at:

[http://www.cisco.com/cgi-bin/tablebuild.pl/ip-7900ser](http://www.cisco.com/cgi-bin/tablebuild.pl/ip-7900ser)

After the phone connects to the network, the phone startup process begins, and the phone registers with Cisco Unified Communications Manager. To complete phone installation, configure the network settings on the phone depending on whether you enable or disable DHCP service.

If you used autoregistration, update the specific configuration information for the phone: associate the phone with a user, change the button table, or assign a directory number.

**Install Cisco Unified IP Phone 7975G, 7971G-GE, 7970G, 7965G, and 7945G**

The following steps provide an overview and checklist of installation tasks for the Cisco Unified IP Phone 7975G, 7971G-GE, 7970G, 7965G, and 7945G. The steps present a suggested order to guide you through the phone installation. Some tasks are optional, depending on your system and user needs. For detailed procedures and information, see the sources in the steps.
Procedure

Step 1  Choose the power source for the phone:
   a) Power over Ethernet (PoE)
   b) External power supply
      Determines how the phone receives power.
      See Cisco Unified IP Phone Power, on page 31.

Step 2  Assemble the phone, adjust phone placement, and connect the network cable.
        Locates and installs the phone in the network.
        See Install Cisco Unified IP Phone, on page 48 and Footstand Adjustment, on page 53.

Step 3  (Optional) Add a Cisco Unified IP Phone Expansion Module.
        Adds the device with its default settings to the Cisco Unified Communications Manager database. Extends
        functionality of a Cisco Unified IP Phone by adding 14 (Cisco Unified IP Phone Expansion Module 7914) or
        24 (Cisco Unified IP Phone Expansion Modules 7915 or 7916) line appearances or speed-dial numbers.
        Note  Cisco Unified IP Phones 7971G-GE and 7970G do not support Cisco Unified IP Phone Expansion
              Modules 7915 and 7916.
        Note  The Cisco Unified IP Phone 7945G does not support any expansion modules.
        Note  A maximum of 56 keys for a Cisco Unified IP Phone 7975G and up to 54 keys for a Cisco Unified
              IP Phone 7965G can be configured.
        See Cisco Unified IP Phone Expansion Module, on page 50.

Step 4  Monitor the phone startup process. Verifies that phone is configured properly.
        See Phone Startup Process, on page 57.

Step 5  When you configure the network settings on the phone, for an IPv4 network you can set up an IP address for
        the phone either by using DHCP or by manually entering an IP address.
        With DHCP: To enable DHCP and allow the DHCP server to automatically assign an IP address to the Cisco
        Unified IP Phone and direct the phone to a TFTP server, choose Settings > Network Configuration > IPv4
        Configuration and configure the following:

            • To enable DHCP, set DHCP Enabled to Yes. DHCP is enabled by default.
            • To use an alternate TFTP server, set Alternate TFTP Server to Yes, and enter the IP address for the
              TFTP Server.
              Note  Consult the network administrator if you need to assign an alternative TFTP server instead of
              using the TFTP server that DHCP assigns.
            • Without DHCP: You must configure the IP address, subnet mask, TFTP server, and default router locally
              on the phone. To do so, choose Settings > Network Configuration > IPv4 Configuration.

        To disable DHCP and manually set an IP address:
        a) Set DHCP Enabled to No.
        b) Enter the static IP address for phone.
        c) Enter the subnet mask.
        d) Enter the default router IP addresses.
        e) Set Alternate TFTP Server to Yes, and enter the IP address for TFTP Server 1.
You must also enter the domain name where the phone resides by choosing **Settings > Network Configuration**.

The Cisco Unified IP Phone supports concurrent IPv4 and IPv6 addresses. You can configure Cisco Unified Communications Manager to support IPv4 addresses only, IPv6 addresses only, or both IPv4 and IPv6 addresses.

See **Network Settings, on page 58** and **Network Configuration Menu, on page 66**.

**Step 6**  
If you configure the network settings on the phone for an IPv6 network, you can set up an IP address for the phone either by using DHCPv6 or by manually entering an IP address.  

With DHCPv6: To enable DHCPv6 and allow the DHCPv6 server to automatically assign an IP address to the Cisco Unified IP Phone and direct the phone to a TFTP server:

- Choose **Settings > Network Configuration > IPv6 Configuration**.
- Set **DHCPv6 Enabled** to **Yes**. DHCPv6 is enabled by default.
- To use an alternate TFTP server, set **IPv6 Alternate TFTP Server** to **Yes** and enter the IP address for **IPv6 TFTP Server 1**.
  
  **Note**  
  Consult the network administrator if you need to assign an alternative TFTP server instead of using the TFTP server that DHCP assigns.

- Without DHCP: You must configure the IP address, subnet mask, TFTP server, and default router locally on the phone, choose **Settings > Network Configuration > IPv6 Configuration**.

To disable DHCP and manually set an IP address:

a) Set **DHCPv6 Enabled** to **No**.

b) Enter the static IP address for phone.

c) Enter the IPv6 prefix length.

d) Set IPv6 Alternate TFTP Server to **Yes**, and enter the IP address for IPv6 TFTP Server 1.

You must also enter the domain name where the phone resides by choosing **Settings > Network Configuration**.

**Note**  
The Cisco Unified IP Phone supports concurrent IPv4 and IPv6 addresses. You can configure Cisco Unified Communications Manager to support IPv4 addresses only, IPv6 addresses only, or both IPv4 and IPv6 addresses.

See **Network Settings, on page 58** and **Network Configuration Menu, on page 66**.

**Step 7**  
Set up security on the phone. Provides protection against data tampering threats and identity theft of phones.  
See **Cisco Unified IP Phone Security, on page 58**.

**Step 8**  
Make calls with the Cisco Unified IP Phone. Verifies that the phone and features work correctly.  
See your phone user guide.

**Step 9**  
Provide information to end users about how to use their phones and how to configure their phone options. Ensures that users have adequate information to use their Cisco Unified IP Phones.  
See **Internal Support Web Site, on page 243**.
Phone and Telephony Network Overview

Cisco Unified IP Phones enable you to communicate by using voice over a data network. To provide this capability, the IP phones depend upon and interact with several other key Cisco Unified IP Telephony and network components, including Cisco Unified Communications Manager, DNS and DHCP servers, TFTP servers, media resources, Cisco PoE, and others.

This chapter focuses on the interactions between the Cisco Unified IP Phone 7975G, 7971G-GE, 7970G, 7965G, and 7945G and Cisco Unified Communications Manager, DNS and DHCP servers, TFTP servers, and switches. It also describes options for powering phones.

For related information about voice and IP communications, see this URL:

This chapter provides an overview of the interaction between the Cisco Unified IP Phone and other key components of the Voice over IP (VoIP) network.

Cisco Unified IP Communications Product Interactions

To function in the IP telephony network, the Cisco Unified IP Phone must be connected to a networking device, such as a Cisco Catalyst switch. You must also register the Cisco Unified IP Phone with a Cisco Unified Communications Manager system before the phone can send and receive calls.
This section includes these topics:

**Cisco Unified IP Phone and Cisco Unified Communications Manager Interactions**

Cisco Unified Communications Manager is an open and industry-standard call processing system. Cisco Unified Communications Manager software sets up and tears down calls between phones, thus integrating traditional PBX functionality with the corporate IP network. Cisco Unified Communications Manager manages the components of the IP telephony system—the phones, the access gateways, and the resources necessary for features such as call conferencing and route planning. Cisco Unified Communications Manager also provides:

- Firmware for phones
- Authentication and encryption (if configured for the telephony system)
- Configuration, CTL, and Identity Trust List (ITL) files via the TFTP service
- Phone registration
- Call preservation, so that a media session continues if signaling is lost between the primary Communications Manager and a phone

For information about configuring Cisco Unified Communications Manager to work with the IP devices described in this chapter, see the *Cisco Unified Communications Manager Administration Guide*, the *Cisco Unified Communications Manager System Guide*, and the *Cisco Unified Communications Manager Security Guide*.

**Note**

If the Cisco Unified IP Phone model that you want to configure does not appear in the Phone Type drop-down list in Cisco Unified Communications Manager Administration, go to the following URL and install the latest support patch for your version of Cisco Unified Communications Manager:


**Related Topics**

- Cisco Unified IP Phone Security Features, on page 13
- Telephony Features Available for Cisco Unified IP Phone, on page 124

**Cisco Unified IP Phone and VLAN Interaction**

The Cisco Unified IP Phone 7975G, 7971G-GE, 7970G, 7965G, and 7945G have an internal Ethernet switch, which enables forwarding of packets to the phone and to the access port and the network port on the back of the phone.

If a computer is connected to the access port, the computer and the phone share the same physical link to the switch and share the same port on the switch. This shared physical link has the following implications for the VLAN configuration on the network:
- The current VLANs might be configured on an IP subnet basis. However, an additional IP address might not be available to assign the phone to the same subnet as other devices connect to the same port.
- Data traffic present on the data/native VLAN may reduce the quality of VoIP traffic.
- Network security may indicate a need to isolate the VLAN voice traffic from the VLAN data traffic.

Resolve these issues by isolating the voice traffic onto a separate VLAN. The switch port to which the phone connects would be configured to have separate VLANs for carrying:

- Voice traffic to and from the IP phone (auxiliary VLAN, on the Cisco Catalyst 6000 series, for example)
- Data traffic to and from the PC that connects to the switch through the access port of the IP phone (native VLAN)

Isolation of the phones on a separate, auxiliary VLAN improves the quality of the voice traffic and allows a large number of phones to be added to an existing network where not enough IP addresses exist for each phone.

For more information, see the documentation included with a Cisco switch. You can also access related documentation at this URL:


**Related Topics**

- Phone Startup Process, on page 36
- Network Configuration Menu, on page 66

---

**Cisco Unified IP Phone Power**

Cisco Unified IP Phone 7975G, 7971G-GE, 7970G, 7965G, and 7945G can be powered with external power or with Power over Ethernet (PoE). A separate power supply provides external power. A switch through the Ethernet cable that is attached to a phone provides PoE.

⚠️ **Caution**

When you install a phone powered with external power, connect the power supply to the phone and to a power outlet before you connect the Ethernet cable to the phone. When you remove a phone that is powered with external power, disconnect the Ethernet cable from the phone before you disconnect the power supply.

The following sections provide more information about phone power:

**Power Guidelines**

The following table provides guidelines that apply to external power and to PoE power for Cisco Unified IP Phone 7975G, 7971G-GE, 7970G, 7965G, and 7945G.
Table 7: Guidelines for Powering the Cisco Unified IP Phone 7975G, 7971G-GE, 7970G, 7965G, and 7945G

<table>
<thead>
<tr>
<th>Power type</th>
<th>Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>External power: Provided through the CP-PWR-CUBE-3 external power supply</td>
<td>The Cisco Unified IP Phone 7975G, 7971G-GE, 7970G, 7965G, and 7945G use the CP-PWR-CUBE-3 power supply.</td>
</tr>
<tr>
<td>External power: Provided through the Cisco Unified IP Phone Power Injector</td>
<td>The Cisco Unified IP Phone Power Injector may be used with any Cisco Unified IP Phone. Functioning as a midspan device, the injector delivers inline power to the attached phone. The Cisco Unified IP Phone Power Injector connects between a switch port and the IP phone, and supports a maximum cable length of 100m between the unpowered switch and the IP phone.</td>
</tr>
</tbody>
</table>
| PoE power: Provided by a switch through the Ethernet cable attached to the phone | The Cisco Unified IP Unified IP Phone 7975G, 7971G-GE, 7970G, 7965G, and 7945G supports IEEE 802.3af Class 3 power on signal pairs and spare pairs.  
To ensure uninterruptible operation of the phone, make sure that the switch has a backup power supply.  
Make sure that the CatOS or IOS version that runs on your switch supports your intended phone deployment. See the documentation for your switch for operating system version information. |

Phone Power Consumption and Display Brightness

The power consumed by a phone depends on its power configuration. The following table provides a power configuration overview with the maximum power consumed by a phone for each configuration option and the correlating phone screen brightness level.

Note: Power consumption values shown in the table include power losses in the cable that connects the phone to the switch.
### Table 8: Power Consumption and Display Brightness for Power Configurations

<table>
<thead>
<tr>
<th>Phone model</th>
<th>Power configuration</th>
<th>Max. power consumed from a switch</th>
<th>Phone screen brightness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified IP Phone 7975G, 7965G, 7945G</td>
<td>IEEE 802.3af Class 3 power from a Cisco switch, with bidirectional power negotiation enabled</td>
<td>12 W</td>
<td>Full</td>
</tr>
<tr>
<td></td>
<td>External power</td>
<td>—</td>
<td>Full</td>
</tr>
<tr>
<td>Cisco Unified IP Phone 7971G-GE</td>
<td>IEEE 802.3af Class 3 power from a Cisco switch (with or without bidirectional power negotiation enabled) or from a third-party switch</td>
<td>15.4 W</td>
<td>Near full</td>
</tr>
<tr>
<td></td>
<td>External power</td>
<td>—</td>
<td>Full</td>
</tr>
<tr>
<td>Cisco Unified IP Phone 7970G</td>
<td>Cisco prestandard PoE from a switch that supports a maximum of 7 W power per port, with bidirectional power negotiation enabled</td>
<td>6.3 W</td>
<td>Approx. 1/2</td>
</tr>
<tr>
<td></td>
<td>Cisco prestandard PoE from a Cisco Switch that supports 7 W or 15.4 W power per port, without bidirectional power negotiation</td>
<td>6.3 W</td>
<td>Approx. 1/2</td>
</tr>
<tr>
<td></td>
<td>IEEE 802.3af Class 3 power from a Cisco switch, without bidirectional power negotiation</td>
<td>6.3 W</td>
<td>Approx. 1/2</td>
</tr>
<tr>
<td></td>
<td>IEEE 802.3af Class 3 power from a third-party switch</td>
<td>6.3 W</td>
<td>Approx. 1/2</td>
</tr>
<tr>
<td></td>
<td>IEEE 802.3af Class 3 power from a Cisco switch, with bidirectional power negotiation enabled</td>
<td>10.25 W</td>
<td>Full (see note)</td>
</tr>
<tr>
<td></td>
<td>Cisco prestandard PoE from a Cisco Switch that supports 15.4 W power per port, with bidirectional power negotiation enabled</td>
<td>10.25 W</td>
<td>Full</td>
</tr>
<tr>
<td></td>
<td>External power</td>
<td>—</td>
<td>Full</td>
</tr>
</tbody>
</table>
Power Outage

Your access to emergency service through the phone requires the phone to receive power. If an interruption in the power supply occurs, Service and Emergency Calling Service dialing do not function until power is restored. In the case of a power failure or disruption, you may need to reset or reconfigure equipment before you can use the Service or Emergency Calling Service dialing.

Additional Information About Power

The documents in the following table provide more information on the following topics:

- Cisco switches that work with the Cisco Unified IP Phone 7975G, 7971G-GE, 7970G, 7965G, and 7945G
- Cisco IOS releases that support bidirectional power negotiation
- Other power requirements and restrictions

<table>
<thead>
<tr>
<th>Document Topics</th>
<th>URL</th>
</tr>
</thead>
</table>

Phone Configuration Files

Phone configuration files are stored on the TFTP server and define Cisco Unified Communications Manager connection parameters. In general, whenever you make a change in Cisco Unified Communications Manager that requires the phone to reset, a change is made automatically to the phone configuration file.
Configuration files also contain information about the image load that the phone should be running. If this image load differs from the one currently that is loaded on a phone currently, the phone contacts the TFTP server to request the required load files. These load files are digitally signed to ensure the authenticity of the file source.

In addition, if the device security mode in the configuration file is set to Authenticated and the CTL file on the phone has a valid certificate for Cisco Unified Communications Manager, the phone establishes a TLS connection to Cisco Unified Communications Manager. Otherwise, the phone establishes a TCP connection. For SIP phones, a TLS connection requires that the transport protocol in the phone configuration file be set to TLS, which corresponds to the transport type in the SIP Security Profile in Cisco Unified Communications Manager Administration.

---

**Note**

If the device security mode in the configuration file is set to Authenticated or Encrypted but the phone has not received a CTL or ITL file, the phone tries four times to obtain the file so it can register securely.

---

**Note**

Cisco Extension Mobility Cross Cluster is an exception, in that the phone permits a TLS connection to Cisco Unified Communications Manager for secure signaling even without the CTL file.

If you configure security-related settings in Cisco Unified Communications Manager Administration, the phone configuration file contains sensitive information. To ensure the privacy of a configuration file, you must configure it for encryption. For more information, see the Cisco Unified Communications Manager Security Guide, "Configuring Encrypted Phone Configuration Files" chapter.

A phone requests a configuration file whenever it resets and registers with Cisco Unified Communications Manager.

A phone accesses a default configuration file named XmlDefault.cnf.xml only when the phone has not received a valid Trust List file that contains a certificate assigned to Cisco Unified Communications Manager and TFTP.

If autoregistration is not enabled and you did not add the phone to the Cisco Unified Communications Manager database, the phone system rejects the phone registration request with Cisco Unified Communications Manager. The phone displays the Configuring IP message continuously until you either enable autoregistration or add the phone to the Cisco Unified Communications Manager database.

If the phone has registered previously, the phone accesses the configuration file named SEPmac_address.cnf.xml, where mac_address is the MAC address of the phone.

For SIP phones, the TFTP server generates these SIP configuration files:

- **SIP IP Phone**
  - For unsigned and unencrypted files: SEP<mac>.cnf.xml
  - For signed files: SEP<mac>.cnf.xml.sgn
  - For signed and encrypted files: SEP<mac>.cnf.xml.enc.sgn

- **Dial Plan:** <dialplan>.xml

- **Softkey Template:** <softkey_template>.xml
The filenames derive from the MAC Address and Description fields in the Phone Configuration window of Cisco Unified Communications Manager. The MAC address uniquely identifies the phone. For more information, see the Cisco Unified Communications Manager Administration Guide.

For more information about the phone interaction with the TFTP server, see the Cisco Unified Communications Manager System Guide, “Cisco TFTP” chapter.

Phone Startup Process

When the Cisco Unified IP Phone connects to the VoIP network, the phone goes through a standard startup process that the following steps describe. Depending on your specific network configuration, not all of these process steps may occur on your Cisco Unified IP Phone.

Procedure

**Step 1** Obtain power from the switch.
If a phone is not using external power, the switch provides in-line power through the Ethernet cable that is attached to the phone.

See Cisco Unified IP Phone Power, on page 31 and Startup Problems, on page 217.

**Step 2** Load the Stored Phone Image.
The Cisco Unified IP Phone has nonvolatile flash memory in which it stores firmware images and user-defined preferences. At startup, the phone runs a bootstrap loader that loads a phone image stored in flash memory. The phone uses this image to initialize its software and hardware.

See Startup Problems, on page 217.

**Step 3** Configure VLAN.
If the Cisco Unified IP Phone is connected to a Cisco switch, the switch next informs the phone of the voice VLAN defined on the switch port. The phone needs to know its VLAN membership before it can proceed with the Dynamic Host Configuration Protocol (DHCP) request for an IP address.

See Network Configuration Menu, on page 66 and Startup Problems, on page 217.

**Step 4** Obtain an IP Address.
If the Cisco Unified IP Phone uses DHCP to obtain an IP address, the phone queries the DHCP server to obtain one. If you do not use DHCP in your network, you must assign static IP addresses to each phone locally.

See Network Configuration Menu, on page 66 and Startup Problems, on page 217.

**Step 5** Access a TFTP Server.
In addition to assigning an IP address, the DHCP server directs the Cisco Unified IP Phone to a TFTP server. If the phone has a statically defined IP address, you must configure the TFTP server locally on the phone. The phone then contacts the TFTP server directly.

*Note* You can also assign an alternative TFTP server to use instead of the one that DHCP assigns.

See Network Configuration Menu, on page 66 and Startup Problems, on page 217.

**Step 6** Request the CTL file.
The TFTP server stores the CTL file. This file contains the certificates that are necessary to establish a secure connection between the phone and Cisco Unified Communications Manager.

See the Cisco Unified Communications Manager Security Guide, “Configuring the Cisco CTL Client” chapter.
Step 7 Request the ITL file.
The phone requests the ITL after it requests the CTL file. The ITL file contains the certificates of the entities that the phone can trust. The certificates are used to authenticate a secure connection with the servers or to authenticate a digital signature that the servers sign.


Step 8 Request the Configuration File.
The TFTP server has configuration files, which define parameters for connecting to Cisco Unified Communications Manager and other information for the phone.

See Phone Configuration Files, on page 34 and Startup Problems, on page 217.

Step 9 Contact Cisco Unified Communications Manager.
The configuration file defines how the Cisco Unified IP Phone communicates with Cisco Unified Communications Manager and provides a phone with the load ID. After the phone obtains the file from the TFTP server, the phone attempts to make a connection to the highest priority Cisco Unified Communications Manager on the list. If the security profile of the phone is configured for secure signaling (encrypted or authenticated), and Cisco Unified Communications Manager is set to secure mode, the phone makes a TLS connection. Otherwise, it makes a nonsecure TCP connection.

If the phone was manually added to the database, Cisco Unified Communications Manager identifies the phone. If the phone was not manually added to the database and autoregistration is enabled in Cisco Unified Communications Manager, the phone attempts to autoregister in the Cisco Unified Communications Manager database.

Note Autoregistration is disabled when you configure the CTL client. In this case, the phone must be manually added to the Cisco Unified Communications Manager database.

See Phone Configuration Files, on page 34 and Startup Problems, on page 217.

---

Cisco Unified Communications Manager Phone Addition Methods

Before you install the Cisco Unified IP Phone, you must choose a method for adding phones to the Cisco Unified Communications Manager database.

The following table provides an overview of the methods for adding phones to the Cisco Unified Communications Manager database.

Table 9: Cisco Unified Communications Manager Phone Addition Methods

<table>
<thead>
<tr>
<th>Method</th>
<th>Requires MAC address?</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autoregistration</td>
<td>No</td>
<td>Results in automatic assignment of directory numbers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Not available when security or encryption is enabled.</td>
</tr>
</tbody>
</table>
## Autoregistration Phone Addition

If you enable autoregistration before you begin installing phones, you can:

- Add phones without first gathering MAC addresses from the phones.
- Automatically add a Cisco Unified IP Phone to the Cisco Unified CM database when you physically connect the phone to your IP telephony network. During autoregistration, Cisco Unified Communications Manager assigns the next available sequential directory number to the phone.
- Quickly enter phones into the Cisco Unified Communications Manager database and modify any settings, such as the directory numbers, from Cisco Unified Communications Manager.
- Move autoregistered phones to new locations and assign them to different device pools without affecting their directory numbers.

### Notes

- Autoregistration is disabled by default. In some cases, you might not want to use autoregistration; for example, if you want to assign a specific directory number to the phone. For information about enabling autoregistration, see "Enable autoregistration" section in the *Cisco Unified Communications Manager Administration Guide*.

<table>
<thead>
<tr>
<th>Method</th>
<th>Requires MAC address?</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autoregistration with TAPS</td>
<td>No</td>
<td>Requires autoregistration and the Bulk Administration Tool (BAT); updates the Cisco Unified Communications Manager database with the MAC address and DNs for the device when user calls TAPS from the phone.</td>
</tr>
<tr>
<td>Use Cisco Unified Communications Manager Administration</td>
<td>Yes</td>
<td>Requires phones to be added individually.</td>
</tr>
<tr>
<td>Use BAT</td>
<td>Yes</td>
<td>Can add groups of same model of phone. Can schedule when phones are added to the Cisco Unified Communications Manager database.</td>
</tr>
</tbody>
</table>

---

**Note**

Cisco recommends that you use autoregistration to add fewer than 100 phones to your network. To add more than 100 phones to your network, use the Bulk Administration Tool (BAT). Autoregistration is disabled by default. In some cases, you might not want to use autoregistration; for example, if you want to assign a specific directory number to the phone. For information about enabling autoregistration, see "Enable autoregistration" section in the *Cisco Unified Communications Manager Administration Guide*.

**Note**

When you configure the cluster for mixed mode through the Cisco CTL client, autoregistration is automatically disabled. When you configure the cluster for nonsecure mode through the Cisco CTL client, autoregistration is automatically enabled.
Autoregistration and TAPS Phone Addition

You can add phones with autoregistration and TAPS, the Tool for Auto-Registered Phones Support, without first gathering MAC addresses from phones.

TAPS works with the Bulk Administration Tool (BAT) to update a batch of phones that were already added to the Cisco Unified Communications Manager database with dummy MAC addresses. Use TAPS to update MAC addresses and download predefined configurations for phones.

Note

Cisco recommends that you use autoregistration and TAPS to add less than 100 phones to your network. To add more than 100 phones to your network, use the Bulk Administration Tool (BAT).

To implement TAPS, dial a TAPS directory number and follow the voice prompts. When the process completes, the phone has downloaded the directory number and other settings, and the phone is updated in Cisco Unified Communications Manager Administration with the correct MAC address.

Autoregistration must be enabled in Cisco Unified Communications Manager Administration (System > Cisco Unified CM) for TAPS to function.

Note

When you configure the cluster for mixed mode through the Cisco CTL client, autoregistration is automatically disabled. When you configure the cluster for nonsecure mode through the Cisco CTL client, autoregistration is automatically enabled.

For more information, see "Bulk Administration" chapter in the Cisco Unified Communications Manager Administration Guide and the "Tool for Auto-Registered Phones Support" chapter in the Cisco Unified Communications Manager Bulk Administration Guide.

Cisco Unified Communications Manager Administration Phone Addition

You can add phones individually to the Cisco Unified Communications Manager database by using Cisco Unified Communications Manager Administration. To do so, you first need to obtain the MAC address for each phone.

After you have collected MAC addresses, in Cisco Unified Communications Manager Administration, choose Device > Phone and click Add New to begin.

For complete instructions and conceptual information about Cisco Unified Communications Manager, see the Cisco Unified Communications Manager Administration Guide and the Cisco Unified Communications Manager System Guide.

Related Topics

Cisco Unified IP Phone MAC Address Determination, on page 41
Add Phones with BAT

Cisco Unified Communications Bulk Administration Tool (BAT), which is a menu option in Cisco Unified Communications Manager Administration, enables you to perform batch operations, which includes registration of multiple phones.

To add phones by using BAT only (not in conjunction with TAPS), you first need to obtain the appropriate MAC address for each phone.

To add a phone to Cisco Unified Communications Manager, follow these steps:

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>From Cisco Unified Communications Manager, choose Bulk Administration &gt; Phones &gt; Phone Template.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click Add New.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Choose a Phone Type and click Next.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Enter the details of phone specific parameters, such as Device Pool, Phone Button Template, and Device Security Profile.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Save.</td>
</tr>
<tr>
<td>Step 6</td>
<td>From Cisco Unified Communications Manager, choose Device &gt; Phone &gt; Add New to add a phone by using an already created BAT phone template. For detailed instructions about using BAT, see the <em>Cisco Unified Communications Manager Bulk Administration Guide</em>. For more information on creation of BAT Phone Templates, see the <em>Cisco Unified Communications Manager Bulk Administration Guide</em>, &quot;Phone Template&quot; chapter.</td>
</tr>
</tbody>
</table>

**Related Topics**

Cisco Unified IP Phone MAC Address Determination, on page 41

Cisco Unified IP Phones and Different Protocols

The Cisco Unified IP Phones can operate with Skinny Client Control Protocol (SCCP) or Session Initiation Protocol (SIP). You can convert a phone from using one protocol to using the other protocol.

Convert New Phone from SCCP to SIP

A new, unused phone is set for SCCP by default. To convert this phone to SIP, perform these steps:

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Take one of these actions:</th>
</tr>
</thead>
<tbody>
<tr>
<td>a)</td>
<td>To autoregister the phone, set the Auto Registration Phone Protocol parameter in Cisco Unified Communications Manager Administration to SIP.</td>
</tr>
</tbody>
</table>
b) To provision the phone by using the Bulk Administration Tool (BAT), choose the appropriate phone model and choose SIP from the BAT.

c) To provision the phone manually, make the appropriate changes for SIP on the Phone configuration window in Cisco Unified Communications Manager Administration.

For more information about Cisco Unified Communications Manager Administration, see the *Cisco Unified Communications Manager Administration Guide*. For more information about BAT, see the *Cisco Unified Communications Manager Bulk Administration Guide*.

**Step 2**  
If you are not using DHCP in your network, configure the network parameters for the phone.

**Step 3**  
Save the configuration updates and perform the following:

a) Click **Apply Config**.

b) When the Apply Configuration Information window displays, click **OK**.

c) Power cycle the phone.

---

**Related Topics**

*Network Settings*, on page 58

---

**In-Use Phone Protocol to Protocol Conversion**

For information on how to convert an in-use phone from one protocol to the other, see the *Cisco Unified Communications Manager Administration Guide*, “Cisco Unified IP Phone Configuration” chapter, “Migrate existing phone settings to another phone” section.

**Deploy Phone in SCCP and SIP Environment**

To deploy Cisco Unified IP Phones in an environment that includes SCCP and SIP and in which the Cisco Unified Communications Manager autoregistration parameter specifies SCCP, perform these general steps:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Set the Cisco Unified Communications Manager <code>auto_registration_protocol</code> parameter to SCCP.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>From Cisco Unified Communications Manager, choose <strong>System &gt; Enterprise Parameters</strong>.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Install the phones.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Change the <strong>Auto Registration Protocol enterprise parameter</strong> to SIP.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Autoregister the SIP phones.</td>
</tr>
</tbody>
</table>

---

**Cisco Unified IP Phone MAC Address Determination**

Several of the procedures in this manual require you to determine the MAC address of a Cisco Unified IP Phone. You can determine the MAC address for a phone in any of these ways:
• From the phone, choose Settings > Network Configuration and view the MAC Address field.
• Look at the MAC label on the back of the phone.
• Display the web page for the phone and click the Device Information hyperlink.

Related Topics
Access Web Page for Phone, on page 200
Phone Installation Overview

This chapter helps you install the Cisco Unified IP Phones on an IP telephony network.

Note

Before you install a Cisco Unified IP Phone, you must decide how to configure the phone in your network. Then you can install the phone and verify the functionality. For more information, see Cisco Unified IP Phones and Telephony Networks, on page 29.

Before You Begin

Before you install the Cisco Unified IP Phone, review the requirements in these sections:
Network Requirements

For the Cisco Unified IP Phone to successfully operate as a Cisco Unified IP Phone endpoint in your network, your network must meet these requirements:

• Working VoIP network:
  ◦ VoIP configured on your Cisco routers and gateways
  ◦ Cisco Unified Communications Manager 4.x and later installed in your network and configured to handle call processing

• IP network that supports DHCP or manual assignment of IP address, gateway, and subnet mask

Note

The Cisco Unified IP Phone displays the date and time from Cisco Unified Communications Manager. The time displayed on the phone can differ from the Cisco Unified Communications Manager time by up to 10 seconds. The Cisco Unified Communications Manager server does not display the local time if it is located in a different time zone than the phones.

Cisco Unified Communications Manager Setup

The Cisco Unified IP Phone requires Cisco Unified Communications Manager to handle call processing. See the Cisco Unified Communications Manager Administration Guide or the context-sensitive help in the Cisco Unified Communications Manager application to ensure that Cisco Unified Communications Manager is set up properly to manage the phone and to properly route and process calls.

If you plan to use autoregistration, verify that it is enabled and properly configured in Cisco Unified Communications Manager before you connect any Cisco Unified IP Phone to the network. For information about enabling and configuring autoregistration, see the Cisco Unified Communications Manager Administration Guide.

You must use Cisco Unified Communications Manager to configure and assign telephony features to the Cisco Unified IP Phones.

In Cisco Unified Communications Manager, you can add users to the database and associate them with specific phones. In this way, users gain access to web pages that allow them to configure items such as call forward, speed dial, and voice message system options.

Related Topics

Cisco Unified Communications Manager User Addition, on page 156
Cisco Unified Communications Manager Phone Addition Methods, on page 37
Telephony Features Available for Cisco Unified IP Phone, on page 124

Cisco Unified IP Phone Components

The Cisco Unified IP Phones include these components on the phone or as accessories for the phone:
Network and Access Ports

The back of the Cisco Unified IP Phones includes these ports:


Each port supports 10/100 or 10/100/1000 Mbps half- or full-duplex connections to external devices.

- For the Cisco Unified IP Phones 7975G, 7971G-GE, and 7970G, you can use either Category 3 or 5 cabling for 10 Mbps connections, but you must use Category 5 for 100 and 1000 Mbps connections (the Cisco Unified IP Phone 7970G does not support 1000 Mbps).
- For the Cisco Unified IP Phones 7965G and 7945G, you can use either Category 3, 5, 5e, or 6 cabling for 10 Mbps connections, but you must use Category 5, 5e, or 6 for 100 Mbps connections.

Use the SW network port to connect the phone to the network. You must use a straight-through cable on this port. The phone can also obtain inline power from a switch over this connection. See Cisco Unified IP Phone Power, on page 31 for details.

Use the PC access port to connect a network device, such as a computer, to the phone. You must use a straight-through cable on this port.

Handset

The handset is designed especially for use with a Cisco Unified IP Phone. The handset includes a light strip to indicate incoming calls and voice messages.

To connect a handset to the Cisco Unified IP Phones 7975G, 7965G, or 7945G, plug the cable into the handset and into the Handset port on the back of the phone.

To connect a handset to the Cisco Unified IP Phones 7971G-GE or 7970G, remove the hookswitch clip from the cradle area, as shown in the following figure. Then plug the cable into the handset and into the Handset port on the back of the phone.

Figure 1: Removing the hookswitch clip

Speakerphone

By default, the speakerphone is enabled on the Cisco Unified IP Phone.
Disable Speakerphone

To disable the speakerphone using Cisco Unified CM Administration, perform the following procedure:

**Procedure**

**Step 1** Choose Device > Phone and locate the phone you want to modify.

**Step 2** In the Phone Configuration window, check Disable Speakerphone.

**Step 3** Click Apply.

Headset

Although Cisco performs internal tests of third-party headsets for use with the Cisco Unified IP Phones, Cisco does not certify or support products from headset or handset vendors.

We recommend the use of good quality external devices, for example, headsets that are screened against unwanted radio frequency (RF) and audio frequency (AF) signals. Depending on the quality of headsets and their proximity to other devices, such as mobile phones and two-way radios, some audio noise or echo may still occur. An audible hum or buzz may be heard by either the remote party or by both the remote party and the Cisco Unified IP Phone user. A range of outside sources can cause humming or buzzing sounds; for example, electric lights, electric motors, or large PC monitors. For more information, see External Device Use, on page 48.

**Note**

In some cases, use of a local power cube or power injector may reduce or eliminate hum.

These environmental and hardware inconsistencies in the locations where Cisco Unified IP Phones are deployed mean that no single headset solution is optimal for all environments.

We recommend that customers test headsets in their intended environment to determine performance prior to purchase and large-scale deployment.

**Note**


Audio Quality

Beyond physical, mechanical, and technical performance, the audio portion of a headset must sound good to the user and the party on the far end. Sound quality is subjective and Cisco cannot guarantee the performance of any headsets or handsets. However, a variety of headsets from leading headset manufacturers have been reported to perform well with Cisco Unified IP Phones.

For additional information, see the Headsets for Cisco Unified IP Phones and Desktop Clients page on Cisco.com.
The Cisco Unified IP Phone 7971G-GE and 7970G do not support wireless headsets.

**Headset Connection**

To connect a headset to the Cisco Unified IP Phone, plug it into the Headset port on the back of the phone. Press the **Headset** button on the phone to place and answer calls by using the headset.

You can use the headset with all Cisco Unified IP Phone features, including the Volume and Mute buttons. Use these buttons to adjust the ear piece volume and to mute the speech path from the headset microphone.

The wireless headset remote hookswitch control feature allows you to use a wireless headset with the Cisco Unified IP Phone. See the wireless headset documentation for information about connecting the headset and using the features.

**Disable Headset**

You can disable the headset by using Cisco Unified Communications Manager Administration.

To disable the headset, perform the following steps:

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose <strong>Device &gt; Phone</strong> and locate the phone you want to modify.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the Phone Configuration window, check the Disable Speakerphone and Headset check box.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click <strong>Apply</strong>.</td>
</tr>
</tbody>
</table>

**Wireless Headset**

The Cisco Unified IP Phones 7971G-GE and 7970G do not support wireless headsets.

By default, the Wireless Headset Hookswitch Control option is disabled. You can enable the option in the Cisco Unified Communications Manager Administration application.

See the wireless headset documentation for information about connecting the headset and using the features.
Enable Headset Hookswitch Control

Procedure

Step 1
Choose Device > Phone and locate the phone you want to modify.

Step 2
In the Phone Configuration window, select Enable for Headset Hookswitch Control.

External Device Use

Cisco recommends the use of good quality external devices, such as speakers, microphones, and headsets that are shielded (screened) against unwanted radio frequency (RF) and audio frequency (AF) signals.

Depending on the quality of these devices and their proximity to other devices, such as mobile phones or two-way radios, some audio noise may still occur. In these cases, Cisco recommends that you take one or more of the following actions:

• Move the external device away from the source of the RF or AF signals.
• Route the external device cables away from the source of the RF or AF signals.
• Use shielded cables for the external device, or use cables with a better shield and connector.
• Shorten the length of the external device cable.
• Apply ferrites or other such devices on the cables for the external device.

Cisco cannot guarantee the performance of the system because Cisco has no control over the quality of external devices, cables, and connectors. The system performs adequately when suitable devices are attached with good quality cables and connectors.

Caution
In European Union countries, use only external headsets that are fully compliant with the EMC Directive [89/336/EC].

Install Cisco Unified IP Phone

You must connect the Cisco Unified IP Phone to the network and to a power source before use. For the description of how to connect the cables to the phone, see Cisco Unified IP Phone Cable Installation, on page 49.

Note
Before you install a phone, even if it is new, upgrade the phone to the current firmware image. Before you use external devices, read External Device Use, on page 48 for safety and performance information.
Before You Begin

Remove the hookswitch clip, if necessary (see Handset, on page 45), from the cradle area.

Procedure

**Step 1**  
Connect the handset to the Handset port.

**Step 2**  
Connect a headset to the Headset port.  
You can add a headset later if you do not connect one now.  
See Headset, on page 46 for supported headsets.

**Step 3**  
Connect a wireless headset. You can add a wireless headset later if you do not want to connect one now.  
*Note*  
The Cisco Unified IP Phones 7971G-GE and 7970G do not support wireless headsets.  
See the wireless headset documentation for information.

**Step 4**  
Connect the power supply to the Cisco DC Adapter port.  
See Cisco Unified IP Phone Power, on page 31.

**Step 5**  
Connect a straight-through Ethernet cable from the switch to the 10/100/1000 SW port on the Cisco Unified IP Phones 7975G and 7971G-GE, or to the 10/100 SW port on the Cisco Unified IP Phones 7970G, 7965G and 7945G.  
Each Cisco Unified IP Phone ships with one Ethernet cable in the box.  
You can use either Category 3/5/5e/6 cabling for 10 Mbps connections, but you must use Category 5/5e/6 for 100 Mbps connections and Category 5e/6 for 1000 Mbps connections.  
See Network and Access Ports, on page 45 for guidelines.

**Step 6**  
Connect a straight-through Ethernet cable from another network device, such as a desktop computer, to the 10/100/1000 PC port on the Cisco Unified IP Phones 7975G and 7971G-GE, or to the 10/100 SW port on the Cisco Unified IP Phones 7970G, 7965G and 7945G.  
You can connect another network device later if you do not connect one now.  
You can use either Category 3/5/5e/6 cabling for 10 Mbps connections, but you must use Category 5/5e/6 for 100 Mbps connections and Category 5e/6 for 1000 Mbps connections.  
See Network and Access Ports, on page 45 for guidelines.

---

**Cisco Unified IP Phone Cable Installation**

See the following figure and table to connect your phone.
Cisco Unified IP Phone Expansion Module

The Cisco Unified IP Phone Expansion Module can be attached to Cisco Unified IP Phone to extend the number of line appearances or speed dial buttons. You can customize the button templates for the Cisco Unified IP Phone Expansion Module to determine the number of line appearances and speed-dial buttons. See the phone button template section for the applicable phone model for details.

Note

The Cisco Unified IP Phones 7971G-GE and 7970G support only the Cisco Unified IP Phone Expansion Module 7914.

Note

The Cisco Unified IP Phone 7945G does not support the Cisco Unified IP Phone Expansion Modules.

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DC adaptor port</td>
<td>2</td>
<td>AC-to-DC power supply</td>
</tr>
<tr>
<td>3</td>
<td>AC power cord</td>
<td>4</td>
<td>Network port</td>
</tr>
<tr>
<td>5</td>
<td>Access port</td>
<td>6</td>
<td>Handset port</td>
</tr>
<tr>
<td>7</td>
<td>Headset port</td>
<td>8</td>
<td>Footstand button</td>
</tr>
<tr>
<td>9</td>
<td>Auxiliary port</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
You can attach one or more Cisco Unified IP Phone Expansion Modules to the Cisco Unified IP Phone 7975G and 7965G by using one of the following methods:

- When you initially add the phone to Cisco Unified Communications Manager, select
  - 7914 14-Button Line Expansion Module for the Cisco Unified IP Phone Expansion 7914
  - 7915 12-Button Line Expansion Module or 7915 24-Button Line Expansion Module for the Cisco Unified IP Phone Expansion Module 7915
  - 7916 12-Button Line Expansion Module or 7916 24-Button Line Expansion Module for the Cisco Unified IP Phone Expansion Module 7916 in the Module 1 or Module 2 fields, and choose the appropriate expansion module firmware. See Step 6, on page 51 in the following procedure.

- Attach the expansion module after the phone is configured in Cisco Unified Communications Manager.

You can attach a Cisco Unified IP Phone Expansion Module 7914 to the Cisco Unified IP Phone 7971G-GE and 7970G by using one of the following methods:

- When you initially add the phone to Cisco Unified Communications Manager, choose 7914 14-Button Line Expansion Module in the Module 1 or Module 2 fields and then choose the appropriate expansion module firmware. See Step 6, on page 51 in the following procedure.

- Attach the expansion module after the phone is configured in Cisco Unified Communications Manager.

**Set up Cisco Unified IP Phone Expansion Module**

To configure the Cisco Unified IP Phone Expansion Module on the Cisco Unified IP Phone, follow these steps:

**Procedure**

**Step 1**
Log in to Cisco Unified Communications Manager Administration.
Cisco Unified Communications Manager Administration displays.

**Step 2**
From the menu, choose Device > Phone.
The Find and List Phone window displays. You can search for one or more phones that you want to configure for the Cisco Unified IP Phone Expansion Module.

**Step 3**
Select and enter your search criteria and click Find.
The Find and List Phone window redisplay and shows a list of the phones that match your search criteria.

**Step 4**
Click the IP phone that you want to configure for the Cisco Unified IP Phone Expansion Module.
The Phone Configuration window displays.

**Step 5**
Scroll to the Expansion Module Information area.

**Step 6**
To add support for one expansion module on Cisco Unified IP Phones 7975G and 7965G, in the Module 1 field, choose one of the following:

- 7914 14-Button Line Expansion Module for the Cisco Unified IP Phone Expansion Module 7914

- 7915 12-Button Line Expansion Module or 7915 24-Button Line Expansion Module for the Cisco Unified IP Phone Expansion Module 7915
To add support for one expansion module on Cisco Unified IP Phones 7971G-GE and 7970G, in the Module 1 field, select **7914 14-Button Line Expansion Module**.

**Step 7**

To add support for a second expansion module on Cisco Unified IP Phones 7975G and 7965G, in the Module 2 field, choose one of the following:

- **7914 14-Button Line Expansion Module** for the Cisco Unified IP Phone Expansion Modules 7914
- **7915 12-Button Line Expansion Module** or **7915 24-Button Line Expansion Module** for the Cisco Unified IP Phone Expansion Module 7915
- **7916 12-Button Line Expansion Module** or **7916 24-Button Line Expansion Module** for the Cisco Unified IP Phone Expansion Module 7916

To add support for a second expansion module on Cisco Unified IP Phones 7971G-GE and 7970G, in the Module 2 field, choose **7914 14-Button Line Expansion Module**.

**Note**

In the Firmware Load Information section, two fields specify the firmware load for Modules 1 and 2. You can leave these fields blank to use the default firmware load.

**Step 8**

Click **Save**.

A message asks you to click the **Apply Config** button for the changes to take effect.

**Step 9**

Click **OK**.

**Step 10**

Click **Apply Config**.

The Apply Configuration Information dialog appears.

**Step 11**

Click **OK**.

**Note**

Refer users to their User Options web pages so they can configure buttons and program buttons to access phone services on the Cisco Unified IP Phone Expansion Module. For more details, see **Phone Features User Subscription and Setup**, on page 245.

---

**Feature Key Capacity Increase for Cisco Unified IP Phones**

The Cisco Unified IP Phone Expansion Modules 7915 and 7916 attach to your Cisco Unified IP Phone 7965G or 7975G and add up to 48 extra line appearances or programmable buttons to your phone. The line capability increase includes Directory Numbers (DN), line information menu, line ring menu, and line help ID. You can configure all 48 additional keys on the Cisco Unified IP Phone Expansion Modules 7915 and 7916.

Use the Phone Button Template Configuration to configure the buttons.

Cisco Unified Communications Manager includes several default phone button templates. When you add phones, you can assign one of these templates to the phones or create a new template.

**Related Topics**

- **Softkey Templates**, on page 155
Set up Additional Buttons

To configure the 48 additional buttons, follow these steps:

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>From Cisco Unified Communications Manager Administration, choose Device &gt; Device Settings &gt; Phone Button Template.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click the Add New button.</td>
</tr>
<tr>
<td>Step 3</td>
<td>From the drop-down list, choose a template and click Copy.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Rename the new template.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Update the template to 56 Directory Numbers for Cisco Unified IP Phone 7975G, or 54 Directory Numbers for Cisco Unified IP Phone 7965G. See the Cisco Unified Communications Manager Administration Guide and the Cisco Unified Communications Manager System Guide for more information about template creation and modification.</td>
</tr>
</tbody>
</table>

**Note** You can also attach two Cisco Unified IP Phone Expansion Modules 7915 units or two Cisco Unified IP Phone Expansion Modules 7916 units to provide 48 additional lines or speed dial and feature buttons.

Footstand Adjustment

The Cisco Unified IP Phone includes an adjustable footstand. When you place the phone on a desktop surface, you can adjust the tilt height to several different angles in 7.5 degree increments from flat to 60 degrees. You can also mount these phones to the wall by using the footstand or by using the optional locking wall mount kit.

To adjust the footstand, push in the footstand adjustment button and adjust the tilt.

Phone Cable Lock

You can secure the Cisco Unified IP Phones to a desktop with a laptop cable lock. The lock connects to the security slot on the back of the phone, and the cable can be secured to a desktop.

The security slot can accommodate a lock that is up to 20 mm wide. Compatible laptop cable locks include the Kensington laptop cable lock and laptop cable locks from other manufacturers that can fit into the security slot on the back of the phone.
Cisco Unified IP Phones 7945G, 7965G, and 7975G Cable Lock

For an illustration on how to connect a cable lock to the Cisco Unified IP Phones 7945G, 7965G, and 7947G, see the following figure.

Figure 2: Connect a Cable Lock
Cisco Unified IP Phones 7970G and 7971G-GE Cable Lock

For an illustration on how to connect a cable lock to the Cisco Unified IP Phones 7970G and 7971G-GE, see the following figure.

**Figure 3: Connect a Cable Lock**

Mount Phone on Wall

You can mount the Cisco Unified IP Phone on the wall by using the footstand as a mounting bracket, or you can use special brackets available in a Cisco Unified IP Phone wall mount kit. Wall mount kits must be ordered separately from the phone.

If you attach the Cisco Unified IP Phone to a wall with the standard footstand and not the wall mount kit, you need to supply the following tools and parts:

- Screwdriver
- Screws to secure the Cisco Unified IP Phone to the wall
See the following figure for a graphical overview of the phone parts.

**Figure 4: Parts Used to Wall Mount the Cisco Unified IP Phone**

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Footstand adjustment button: Raises and lowers adjustment plate</td>
</tr>
<tr>
<td>2</td>
<td>Wall mounting screw holes</td>
</tr>
<tr>
<td>3</td>
<td>Adjustment plate: Raises and lowers phone vertically</td>
</tr>
</tbody>
</table>

**Before You Begin**

To ensure that the handset attaches securely to a wall-mounted phone, remove the handset wall hook from the handset rest, rotate the hook 180 degrees, and reinsert the hook. Turning the hook exposes a lip on which the handset catches when the phone is vertical. For an illustrated procedure, see Installing the Wall Mount Kit for the Cisco Unified IP Phone at:


---

**Caution**

Use care not to damage wires or pipes located inside the wall when securing screws to wall studs.

**Procedure**

**Step 1** Push in the footstand adjustment button.

**Step 2** Adjust the footstand, so it is flat against the back of the phone.

**Step 3** Insert two screws into a wall stud, matching them to the two screw holes on the back of the footstand. The keyholes fit standard phone jack mounts.

**Step 4** Hang the phone on the wall.
Phone Startup Process

After the Cisco Unified IP Phone has power connected to it, the phone begins its startup process by cycling through these steps.

1. These buttons flash on and off in sequence:
   - Headset (Only if the handset is off-hook when the phone powers up. In this case, hang up the handset within 3 seconds or the phone launches its secondary load instead of its primary load.)
   - Mute
   - Speaker

2. Some or all of the line keys flash orange.

Caution

If the line keys flash red in sequence after flashing yellow, do not power down the phone until the sequence of red flashes completes. This sequence can take several minutes to complete.

3. Some or all of the line keys flash green.

   Normally, this sequence takes just a few seconds. However, if the phone flash memory is erased or the phone load is corrupted, the sequence of green flashes will continue while the phone begins a software update procedure. If the phone performs this procedure, the following buttons light to indicate progress:
   - Headset: Phone is waiting for the network and completing CDP and DHCP configuration. A DHCP server must be available in your network.
   - Mute: Phone is downloading images from the TFTP server.
   - Speaker: Phone is writing images to its flash memory.


5. These messages display as the phone starts:
   - Verifying load (if the phone load does not match the load on the TFTP server). If this message displays, the phone start up again and repeats step 1 through step 4 above.
   - Configuring IP
   - Updating the Trust List
   - Updating Locale
   - Configuring Unified CM List
   - Registering

6. The main phone screen displays:
   - Current date and time
   - Primary directory number
   - Additional directory numbers and speed dial numbers, if configured
If the phone successfully passes through these stages, it has started up properly. If the phone does not start up properly, see `Startup Problems`, on page 217.

**Network Settings**

If you are not using DHCP in your network, you must configure these network settings on the Cisco Unified IP Phone after you install the phone on the network:

- IP address
- IP subnet information (subnet mask for IPv4 and subnet prefix length for IPv6)
- Default gateway IP address
- TFTP server IP address

You may also configure these optional settings as necessary:

- Domain name
- DNS server IP address

**Related Topics**

Cisco Unified IP Phone Settings, on page 61

**Cisco Unified IP Phone Security**

The security features protect against several threats, including threats to the identity of the phone and to data. These features establish and maintain authenticated communication streams between the phone and the Cisco Unified Communications Manager server, and digitally sign files before they are delivered.

For more information about the security features, see `Cisco Unified Communications Manager Security Guide`.

**Related Topics**

Cisco Unified IP Phone Security Features, on page 13

**Supported TLS and Ciphers**

TLS v1.0

Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
Install Locally Significant Certificate

You can initiate the installation of a Locally Significant Certificate (LSC) from the Security Configuration menu on the phone. This menu also lets you update or remove an LSC.

If you use a Third Party CA to sign LSCs, note that the Cisco Unified IP Phone 7900 Series only support SHA-1 as the algorithm to sign certificates. The phones do not support SHA-2 (SHA256). For more information on the use of a Third Party CA to sign LSCs, see CUCM Third-Party CA-Signed LSCs Generation and Import Configuration Example in https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/118779-configure-cucm-00.html.

Depending on how you have configured the CAPF, this procedure installs an LSC, updates an existing LSC, or removes an existing LSC.

Before You Begin

Make sure that the appropriate Cisco Unified Communications Manager and the Certificate Authority Proxy Function (CAPF) security configurations are complete:

- The CTL file or ITL file should have a CAPF certificate.
- On Cisco Unified Communications Operating System Administration, verify that the CAPF certificate has been installed.
- The CAPF is running and configured.

For more information, see Cisco Unified Communications Manager Security Guide.

Procedure

Step 1

Obtain the CAPF authentication code that was set when the CAPF was configured.

Step 2

From the phone, press the Settings > Security Configuration.

Note: You can control access to the Settings Menu by using the Settings Access field in the Cisco Unified Communications Manager Administration Phone Configuration window. For more information, see Cisco Unified Communications Manager Administration Guide.

Step 3

Press **# to unlock settings on the Security Configuration menu. See Unlock and Lock Options, on page 63 for information about using locking and unlocking options.

Note: If a Settings Menu password has been set up, SIP phones present an Enter password prompt after you enter **#.

Step 4

Scroll to LSC and press Update.

The phone prompts for an authentication string.

Step 5

Enter the authentication code and press Submit.

The phone begins to install, update, or remove the LSC, depending on how the CAPF was configured. During the procedure, a series of messages displays in the LSC option field in the Security Configuration menu so you can monitor progress. When the procedure completes successfully, the phone displays Installed or Not Installed.

The LSC install, update, or removal process can take a long time to complete. To stop the process at any time, press the Stop softkey from the Security Configuration menu. (Settings must be unlocked before you can press this softkey.)
When the phone successfully completes the installation procedure, it displays Success. If the phone displays Failure, the authorization string may be incorrect or the phone may not be enabled for upgrade. Investigate the error messages that the CAPF generates and take appropriate actions.

To verify that an LSC is installed on the phone, choose **Settings > Model Information** and ensure that the LSC setting shows Installed.

**Related Topics**

Cisco Unified IP Phone Security Features, on page 13
Cisco Unified IP Phone Settings

- Phone Settings Overview, page 61
- Cisco Unified IP Phone Menus, page 61
- Phone Setup Options, page 64
- Network Configuration Menu, page 66
- Device Configuration Menu, page 85
- Security Configuration Menu, page 109

Phone Settings Overview

The Cisco Unified IP Phone includes many configurable network and device settings that you may need to modify before the phone is functional for your users. You can access these settings, and change many of them, through menus on the phone.

Cisco Unified IP Phone Menus

The Cisco Unified IP Phone includes the following configuration menus:

- Network Configuration menu: Provides options for viewing and modifying various network settings.
- Device Configuration menu: Provides access to submenus from which you can view various settings that are not network related.
- Security Configuration menu: Provides options for displaying and modifying security settings.

Before you can change option settings on the Network Configuration menu, you must unlock options for edit. See Unlock and Lock Options, on page 63 for instructions.

For information about the keys you can use to edit or change option settings, see Value Input Guidelines, on page 63.

To control whether a phone user has access to phone settings, use the Settings Access field in the Cisco Unified Communications Manager Administration Phone Configuration window.
To display a configuration menu, perform the following steps.

**Note**

To control whether a phone has access to the Settings menu or to options on this menu, use the Settings Access field in the Cisco Unified Communications Manager Administration Phone Configuration window. The Settings Access field accepts these values:

- **Enabled:** Allows access to the Settings menu.
- **Disabled:** Prevents access to the Settings menu.
- **Restricted:** Allows access to the User Preferences menu and allows volume changes to be saved. Prevents access to other options on the Settings menu.

If you cannot access an option on the Settings menu, check the Settings Access field.

**Procedure**

**Step 1** Press the **Settings** button to access the Settings menu.

**Step 2** Perform one of these actions to display the desired menu:

a) Use the **Navigation** button to select the desired menu and then press **Select**.

b) Use the keypad on the phone to enter the number that corresponds to the menu.

**Step 3** To display a submenu, repeat Step 2.

**Step 4** To exit a menu, press **Exit**.

**Related Topics**

Unlock and Lock Options, on page 63
Value Input Guidelines, on page 63
Phone Setup Options, on page 64
Network Configuration Menu, on page 66
Device Configuration Menu, on page 85
Security Configuration Menu, on page 109
Unlock and Lock Options

Configuration options that can be changed from a phone are locked by default to prevent users from making changes that could affect the operation of a phone. You must unlock these options before you can change them.

When options are inaccessible for modification, a locked padlock icon appears on the configuration menus. When options are unlocked and accessible for modification, an unlocked padlock icon appears on these menus.

To unlock or lock options, press **#. This action either locks or unlocks the options, depending on the previous state.

- **Note**
  If a Settings Menu password has been provisioned, SIP phones present an “Enter password” prompt after you enter **#**.

- **Make sure to lock options after you have made your changes.**

- **Caution**
  Do not press **#** to unlock options and then immediately press **#** again to lock options. The phone will interpret this sequence as **##**, which will reset the phone. To lock options after you unlock them, wait at least 10 seconds before you press **#** again.

Related Topics

- Display Settings Menu, on page 62
- Value Input Guidelines, on page 63
- Phone Setup Options, on page 64
- Network Configuration Menu, on page 66
- Device Configuration Menu, on page 85

Value Input Guidelines

When you edit the value of an option setting, follow these guidelines:

- 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.

- To enter a period (for example, in an IP address under IPv4 Configuration), press the . (period) softkey or press * on the keypad.

- To enter a colon (for example, in an IP address under IPv6 Configuration), press the : (colon) softkey or press * on the keypad.

- Press the << softkey if you make a mistake. This softkey deletes the character to the left of the cursor.
• Press the **Cancel** softkey before you press the **Save** softkey to discard any changes that you have made.

**Note**
The Cisco Unified IP Phone provides several methods you can use to reset or restore option settings, if necessary. For more information, see Cisco Unified IP Phone Reset or Restore, on page 236.

**Related Topics**
- Display Settings Menu, on page 62
- Unlock and Lock Options, on page 63
- Phone Setup Options, on page 64
- Network Configuration Menu, on page 66
- Device Configuration Menu, on page 85
- Security Configuration Menu, on page 109

**Phone Setup Options**

The settings that you can change on a phone fall into several categories, as shown in the following table. For a detailed explanation of each setting and instructions for changing them, see Network Configuration Menu, on page 66.

**Note**
Several options on various configuration menus are for display only, or you can configure these options from Cisco Unified Communications Manager. This chapter also describes these options.

**Table 10: Settings Configurable from the Phone**

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Network Configuration menu option</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Network Settings</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VLAN settings</td>
<td>Admin. VLAN ID allows you to change the administrative VLAN used by the phone. PC VLAN allows the phone to interoperate with third-party switches that do not support a voice VLAN.</td>
<td>Admin. VLAN ID PC VLAN</td>
</tr>
<tr>
<td>Port settings</td>
<td>Allow you to set the speed and duplex of the network and access ports.</td>
<td>SW Port Configuration PC Port Configuration</td>
</tr>
<tr>
<td><strong>IPv4 Network Settings</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>Description</td>
<td>Network Configuration menu option</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td><strong>DHCP settings</strong></td>
<td>Dynamic Host Configuration Protocol (DHCP) automatically assigns IP address to devices when you connect them to the network. Cisco Unified IP Phones enable DHCP by default.</td>
<td>DHCP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DHCP Address Released</td>
</tr>
<tr>
<td><strong>IP settings</strong></td>
<td>If you do not use DHCP in your network, you can make IP settings manually.</td>
<td>Domain Name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IP Address</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Subnet Mask</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default Router 1-5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DNS Server 1-5</td>
</tr>
<tr>
<td><strong>TFTP settings for TFTP IPv4 servers</strong></td>
<td>If you do not use DHCP to direct the phone to a TFTP server, you must manually assign a TFTP server. You can also assign an alternative TFTP server to use instead of the one assigned by DHCP.</td>
<td>TFTP Server 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Alternate TFTP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TFTP Server 2</td>
</tr>
<tr>
<td><strong>IPv6 Network Settings</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>DHCP settings</strong></td>
<td>Dynamic Host Configuration Protocol (DHCP) automatically assigns IP address to phone when you connect them to the network. Cisco Unified IP Phones enable DHCP by default.</td>
<td>DHCPv6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DHCPv6 Address Released</td>
</tr>
<tr>
<td><strong>IP settings</strong></td>
<td>If you do not use DHCP in your network, you can make IP settings manually.</td>
<td>Domain Name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IPv6 Address</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IPv6 Prefix Length</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IPv6 DNS Server 1-2</td>
</tr>
<tr>
<td><strong>TFTP settings for TFTP IPv6 servers (SCCP phones only)</strong></td>
<td>If you do not use DHCP to direct the phone to a TFTP server, you must manually assign a TFTP server. You can also assign an alternative TFTP server to use instead of the one that DHCP assigns.</td>
<td>IPv6 TFTP Server 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IPv6 Alternate TFTP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IPv6 TFTP Server 2</td>
</tr>
</tbody>
</table>

**Related Topics**

Display Settings Menu, on page 62
Network Configuration Menu

The Network Configuration menu provides options for viewing and modifying various network settings. The following tables describe these options and, where applicable, explains how to change them.

For information about how to access the Network Configuration menu, see Display Settings Menu, on page 62.

Note: The phone also has a Network Configuration menu that you access directly from the Settings menu. For information about the options on that menu, see Network Configuration Menu, on page 103.

Before you can change an option on this menu, you must unlock options as described in Unlock and Lock Options, on page 63. The Edit, Yes, or No softkeys for modifying network configuration options appear only if options are unlocked.

For information about the keys you can use to edit options, see Value Input Guidelines, on page 63.

Table 11: Network Configuration Menu Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To Change</th>
</tr>
</thead>
</table>
| IPv4 Configuration | Internet Protocol v4 address menu. In the IPv4 Configuration menu, you can do the following:  
• Enable or disable the phone to use the IPv4 address that is assigned by the DHCPv4 server.  
• Manually set the IPv4 Address, Subnet Mask, Default Routers, DNSv4 Server, and Alternate TFTP servers for IPv4.  
For more information on the IPv4 address fields, refer to the specific field within this table. | Set IPv4 Configuration Fields, on page 75 |
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To Change</th>
</tr>
</thead>
</table>
| IPv6 Configuration | Internet Protocol v6 address menu. In the IPv6 Configuration menu, you can do the following:  
  • Enable or disable the phone to use the IPv6 address that is assigned by the DHCPv6 server, or to use the IPv6 address that the phone acquires through Stateless Address Autoconfiguration (SLAAC).  
  • Manually set the IPv6 Address, Subnet Prefix Length, Default Routers, DNSv6 Server, and IPv6 TFTP servers.  
  For more information on the IPv6 address fields, see DHCPv6 and Autoconfiguration, on page 84.  
  For more information on SLAAC, see Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager at the following location: http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/ipv6/ipv6srnd.html | Set IPv6 Configuration Fields, on page 76 |
| MAC Address        | Unique Media Access Control (MAC) address of the phone.                       | Display only. Cannot configure.                                           |
| Host Name          | Unique host name that the DHCP server assigned to the phone.                 | Display only. Cannot configure.                                           |
| Domain Name        | Name of the Domain Name System (DNS) domain in which the phone resides.      | Set Domain Name Field, on page 76                                         |
  **Note**           | If the phone receives different domain names from the DHCPv4 and DHCPv6 servers, the domain name from the DHCPv6 will take precedence. |                                                             |
| Operational VLAN ID| Auxiliary Virtual Local Area Network (VLAN) configured on a Cisco Catalyst switch in which the phone is a member.  
  If the phone has not received an auxiliary VLAN, this option indicates the Administrative VLAN.  
  If neither the auxiliary VLAN nor the Administrative VLAN are configured, this option is blank.  
  The phone obtains its Operational VLAN ID from Cisco Discovery Protocol (CDP) from the switch to which the phone is attached. To assign a VLAN ID manually, use the Admin VLAN ID option. |                                                             |
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin. VLAN ID</td>
<td>Auxiliary VLAN in which the phone is a member. Used only if the phone does not receive an auxiliary VLAN from the switch; otherwise it is ignored.</td>
<td>Set Admin VLAN ID Field, on page 77</td>
</tr>
<tr>
<td>SW Port Configuration</td>
<td>Speed and duplex of the network port. Valid values:</td>
<td>Set SW Port Configuration Field, on page 77</td>
</tr>
<tr>
<td></td>
<td>• Auto Negotiate</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 10 Half—10-BaseT/half duplex</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 10 Full—10-BaseT/full duplex</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 100 Half—100-BaseT/half duplex</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 100 Full—100-BaseT/full duplex</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1000 Full—1000-BaseT/full duplex</td>
<td></td>
</tr>
<tr>
<td></td>
<td>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 auto-negotiate.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If you change the setting of this option, you must change the PC Port Configuration option to the same setting.</td>
<td></td>
</tr>
<tr>
<td>PC Port Configuration</td>
<td>Speed and duplex of the access port. Valid values:</td>
<td>Set PC Port Configuration Field, on page 77</td>
</tr>
<tr>
<td></td>
<td>• Auto Negotiate</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 10 Half—10-BaseT/half duplex</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 10 Full—10-BaseT/full duplex</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 100 Half—100-BaseT/half duplex</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 100 Full—100-BaseT/full duplex</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1000 Full—1000-BaseT/full duplex</td>
<td></td>
</tr>
<tr>
<td></td>
<td>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 auto-negotiate.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If you change the setting of this option, you must change the SW Port Configuration option to the same setting.</td>
<td></td>
</tr>
</tbody>
</table>
To change Description Option

Set PC VLAN Field, on page 78

Allows the phone to interoperate with third-party switches that do not support a voice VLAN. The Admin VLAN ID option must be set before you can change this option.

PC VLAN

Display only. Cannot configure. Shows the VPN (virtual private network) Client state:
• Connected
• Not Connected

(Supported only for the Cisco Unified IP Phone 7945G, 7965G, and 7975G.)

VPN

The following table describes the IPv4 Configuration menu options.

Table 12: IPv4 Configuration menu options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP</td>
<td>Indicates whether the phone has DHCP enabled or disabled.</td>
<td>Set DHCP Field, on page 78</td>
</tr>
<tr>
<td></td>
<td>When DHCP is enabled, the DHCP server assigns the phone an IPv4 address.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>When DHCP is disabled, the administrator must manually assign an IPv4 address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>to the phone.</td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>Internet Protocol version 4 (IPv4) address of the phone.</td>
<td>Set IP Address Field, on page 78</td>
</tr>
<tr>
<td></td>
<td>If you assign an IPv4 address with this option, you must also assign a subnet</td>
<td></td>
</tr>
<tr>
<td></td>
<td>mask and default router.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>See Subnet Mask and Default Router 1 options in this table.</td>
<td></td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Subnet mask used by the phone.</td>
<td>Set Subnet Mask Field, on page 79</td>
</tr>
<tr>
<td>Default Router 1</td>
<td>Default router used by the phone (Default Router 1) and optional backup routers (Default Router 2–5).</td>
<td>Set Default Router Fields, on page 79</td>
</tr>
<tr>
<td>Default Router 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Default Router 3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Default Router 4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Default Router 5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>To change</td>
</tr>
<tr>
<td>-----------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>DNS Server 1</td>
<td>Primary Domain Name System (DNS) server (DNS Server 1) and optional backup DNS servers (DNS Server 2–5) that the phone uses.</td>
<td>Set DNS Server Fields, on page 79</td>
</tr>
<tr>
<td>DNS Server 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Server 3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Server 4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Server 5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHCP Address Released</td>
<td>Releases the IPv4 IP address that DHCP assigns.</td>
<td>Set DHCP Field, on page 78</td>
</tr>
<tr>
<td>DHCP Server</td>
<td>IP address of the Dynamic Host Configuration Protocol (DHCP) server from which the phone obtains its IPv4 address.</td>
<td>Display only. Cannot configure.</td>
</tr>
<tr>
<td>Alternate TFTP</td>
<td>Indicates whether the phone uses an alternative TFTP server.</td>
<td>Set Alternate TFTP Field, on page 80</td>
</tr>
</tbody>
</table>
To change Description Option

**Set TFTPServer1 Field, on page 80**

### Primary Trivial File Transfer Protocol (TFTP) server that the phone uses. If you are not using DHCP in your network and you want to change this server, you must use the TFTPServer1 option.

If you set the Alternate TFTP option to Yes, you must enter a nonzero value for the TFTPServer1 option.

If neither the primary TFTP server nor the backup TFTP server is listed in the CTL or ITL file on the phone, you must unlock the file before you can save changes to the TFTPServer1 option. In this case, the phone deletes the file when you save changes to the TFTPServer1 option. A new CTL or ITL file will be downloaded from the new TFTPServer1 address.

When the phone looks for its TFTP server, it gives precedence to manually assigned TFTP servers, regardless of the protocol. If your configuration includes both IPv6 and IPv4 TFTP servers, the phone prioritizes the order that it looks for its TFTP server by giving priority to manually assigned IPv6 TFTP servers and IPv4 TFTP servers. The phone looks for its TFTP server in the following order:

1. Any manually assigned IPv6 TFTP servers
2. Any manually assigned IPv4 TFTP servers
3. DHCPv6 assigned TFTP servers
4. DHCP assigned TFTP servers

**Note** For information about the CTL and ITL files, see the *Cisco Unified Communications Manager Security Guide*. For information about unlocking the CTL or ITL files, see **Unlock CTL and ITL Files, on page 113**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
<tbody>
<tr>
<td>TFTPServer1</td>
<td>Primary Trivial File Transfer Protocol (TFTP) server that the phone uses.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If you are not using DHCP in your network and you want to change this server, you must use the TFTPServer1 option.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If you set the Alternate TFTP option to Yes, you must enter a nonzero value for the TFTPServer1 option.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If neither the primary TFTP server nor the backup TFTP server is listed in the CTL or ITL file on the phone, you must unlock the file before you can save changes to the TFTPServer1 option. In this case, the phone deletes the file when you save changes to the TFTPServer1 option. A new CTL or ITL file will be downloaded from the new TFTPServer1 address.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>When the phone looks for its TFTP server, it gives precedence to manually assigned TFTP servers, regardless of the protocol. If your configuration includes both IPv6 and IPv4 TFTP servers, the phone prioritizes the order that it looks for its TFTP server by giving priority to manually assigned IPv6 TFTP servers and IPv4 TFTP servers. The phone looks for its TFTP server in the following order:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1. Any manually assigned IPv6 TFTP servers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Any manually assigned IPv4 TFTP servers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. DHCPv6 assigned TFTP servers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. DHCP assigned TFTP servers</td>
<td></td>
</tr>
</tbody>
</table>

**Note** For information about the CTL and ITL files, see the *Cisco Unified Communications Manager Security Guide*. For information about unlocking the CTL or ITL files, see **Unlock CTL and ITL Files, on page 113**.
To change Description Option

Set TFTPServer2 Field, on page 81

Optional backup TFTPServer that the phone uses if the primary TFTPServer is unavailable.

If neither the primary TFTPServer nor the backup TFTPServer is listed in the CTL or ITL file on the phone, you must unlock either of the files before you can save changes to the TFTPServer 2 option. In this case, the phone deletes either of the files when you save changes to the TFTPServer 2 option. A new CTL or ITL file will be downloaded from the new TFTPServer 2 address.

When the phone looks for its TFTPServer, it gives precedence to manually assigned TFTPServers, regardless of the protocol. If your configuration includes both IPv6 and IPv4 TFTPServers, the phone prioritizes the order that it looks for its TFTPServer by giving priority to manually assigned IPv6 TFTPServers and IPv4 TFTPServers. The phone looks for its TFTPServer in the following order:

1. Manually assigned IPv6 TFTPServers
2. Manually assigned IPv4 TFTPServers
3. DHCPv6 assigned TFTPServers
4. DHCP assigned TFTPServers

**Note** For information about the CTL or ITL file, see the Cisco Unified Communications Manager Security Guide. For information about unlocking the CTL and ITL files, see Unlock CTL and ITL Files, on page 113.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
<tbody>
<tr>
<td>TFTPServer 2</td>
<td>Optional backup TFTPServer that the phone uses if the primary TFTPServer is unavailable.</td>
<td>Set TFTPServer 2 Field, on page 81</td>
</tr>
<tr>
<td>BOOTP Server</td>
<td>Indicates whether the phone obtains its configuration from a Bootstrap Protocol (BootP) server instead of from a DHCP server.</td>
<td>Display only. Cannot configure.</td>
</tr>
</tbody>
</table>

The following table describes the IPv6 Configuration menu options.
### Table 13: IPv6 Configuration menu options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCPv6</td>
<td>Indicates whether the phone has DHCP enabled or disabled. When DHCPv6 is enabled, the DHCPv6 server assigns the phone an IPv6 address. When DHCPv6 is disabled, the administrator must manually assign an IPv6 address to the phone. The DHCPv6 setting along with the Auto IP Configuration setting determine how the IP phone obtains its network settings. For more information on how these two settings affect the network settings on the phone, see DHCPv6 and Autoconfiguration, on page 84.</td>
<td>Set DHCPv6 Field, on page 81</td>
</tr>
<tr>
<td>IPv6 Address</td>
<td>Internet Protocol version 6 (IPv6) address of the phone. The IPv6 address is a 128 bit address. If you assign an IP address with this option, you must also assign the IPv6 prefix length and default router. See IPv6 Prefix Length in this table.</td>
<td>Set IPv6 Address Field, on page 81</td>
</tr>
<tr>
<td>IPv6 Prefix Length</td>
<td>Subnet prefix length that is used by the phone. The subnet prefix length is a decimal value from 1 to 128, that specifies the portion of the IPv6 address that comprises the subnet.</td>
<td>Set IPv6 Prefix Length Field, on page 82</td>
</tr>
<tr>
<td>IPv6 Default Router 1</td>
<td>Default router used by the phone (Default Router 1). Note: The phone obtains information on the default router from IPv6 Router Advertisements.</td>
<td>Set IPv6 Default Router 1 Field, on page 82</td>
</tr>
<tr>
<td>IPv6 DNS Server 1</td>
<td>Primary Domain Name System (DNS) server (DNS Server 1) and optional backup DNS servers (DNS Server 2) used by the phone. If your configuration includes both DNSv6 and DNSv4 servers, the phone will look for its DNS server in the following order: 1 IPv6 DNS Server 1 2 IPv6 DNS Server 2 3 DNS Server 1-5 for IPv4 (respectively)</td>
<td>Set IPv6 DNS Server 1 and IPv6 DNS Server 2 Fields, on page 82</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>To change</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DHCPv6 Address Released</td>
<td>Releases the IPv6 address that the phone has acquired from the DHCPv6 server or by stateless address auto configuration. Note: This field is only editable when the DHCPv6 option is enabled.</td>
<td>Set DHCPv6 Address Released Field, on page 83</td>
</tr>
<tr>
<td>IPv6 Alternate TFTP</td>
<td>Indicates whether the phone is using the IPv6 Alternate TFTP server.</td>
<td>Set IPv6 Alternate TFTP Field, on page 83</td>
</tr>
<tr>
<td>IPv6 TFTP Server 1 (SCCP phones only)</td>
<td>Primary IPv6 Trivial File Transfer Protocol (TFTP) server used by the phone. If you are not using DHCPv6 in your network and you want to change this server, you must use the IPv6 TFTP Server 1 option. If you set the IPv6 Alternate TFTP option to Yes or you disable DHCPv6, you must enter a non-zero value for the IPv6 TFTP Server 1 option. If you make changes to the Alternate TFTP or IPv6 TFTP servers, you must first unlock the CTL or ITL file on the phone. When the phone looks for its TFTP server, it gives precedence to manually assigned TFTP servers, regardless of the protocol. If your configuration includes both IPv6 and IPv4 TFTP servers, the phone prioritizes the order that it looks for its TFTP server by giving priority to manually assigned IPv6 TFTP servers and IPv4 TFTP servers. The phone looks for its TFTP server in the following order: 1. Manually assigned IPv6 TFTP servers 2. Manually assigned IPv4 TFTP servers 3. DHCPv6 assigned TFTP servers 4. DHCP assigned TFTP servers For information about the CTL or ITL file, see the Cisco Unified Communications Manager Security Guide. For information about unlocking CTL files, see Unlock CTL and ITL Files, on page 113.</td>
<td>Set IPv6 TFTP Server 1 Field, on page 83</td>
</tr>
</tbody>
</table>
**IPv6 TFTP Server 2 (SCCP phones only)**

Optional backup IPv6 TFTP server that the phone uses if the primary IPv6 TFTP server is unavailable.

If you make changes to the Alternate TFTP or IPv6 TFTP servers, you must first unlock the CTL or ITL file on the phone.

When the phone looks for its TFTP server, it gives precedence to manually assigned TFTP servers, regardless of the protocol. If your configuration includes both IPv6 and IPv4 TFTP servers, the phone prioritizes the order that it looks for its TFTP server by giving priority to manually assigned IPv6 TFTP servers and IPv4 TFTP servers. The phone looks for the TFTP server in the following order:

1. Manually assigned IPv6 TFTP servers
2. Manually assigned IPv4 TFTP servers
3. DHCPv6 assigned TFTP servers
4. DHCP assigned TFTP servers

For information about the CTL or ITL file, see the *Cisco Unified Communications Manager Security Guide*. For information about unlocking CTL or ITL files, see to Unlock CTL and ITL Files, on page 113.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 TFTP Server 2 (SCCP phones only)</td>
<td>Optional backup IPv6 TFTP server that the phone uses if the primary IPv6 TFTP server is unavailable. If you make changes to the Alternate TFTP or IPv6 TFTP servers, you must first unlock the CTL or ITL file on the phone. When the phone looks for its TFTP server, it gives precedence to manually assigned TFTP servers, regardless of the protocol. If your configuration includes both IPv6 and IPv4 TFTP servers, the phone prioritizes the order that it looks for its TFTP server by giving priority to manually assigned IPv6 TFTP servers and IPv4 TFTP servers. The phone looks for the TFTP server in the following order: 1. Manually assigned IPv6 TFTP servers 2. Manually assigned IPv4 TFTP servers 3. DHCPv6 assigned TFTP servers 4. DHCP assigned TFTP servers</td>
<td>Set IPv6 TFTP Server 2 Field, on page 84</td>
</tr>
</tbody>
</table>

### Set IPv4 Configuration Fields

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Unlock network configuration options.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Scroll to IPv4 Configuration and press the <strong>Select</strong> softkey.</td>
</tr>
</tbody>
</table>
Set IPv6 Configuration Fields

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Unlock network configuration options.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Scroll to IPv6 Configuration and press the Select softkey.</td>
</tr>
</tbody>
</table>

Set Domain Name Field

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Unlock network configuration options.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>To disable DHCP, perform one of the following actions:</td>
</tr>
<tr>
<td></td>
<td>• If the IP Addressing mode is configured for IPv4 only, set the DHCP option to No.</td>
</tr>
<tr>
<td></td>
<td>• If the IP Addressing mode is configured for IPv6 only, set the DHCPv6 option to No.</td>
</tr>
<tr>
<td></td>
<td>• If the IP Addressing mode is configured for both IPv4 and IPv6, set both DHCP option and DHCPv6 to No.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Scroll to the Domain Name option.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Press Edit.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Enter a new domain name.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Press Validate.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Press Save.</td>
</tr>
</tbody>
</table>
Set Admin VLAN ID Field

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Unlock network configuration options.</td>
</tr>
<tr>
<td>2</td>
<td>Scroll to the Admin. VLAN ID option.</td>
</tr>
<tr>
<td>3</td>
<td>Press <strong>Edit</strong>.</td>
</tr>
<tr>
<td>4</td>
<td>Enter a new Admin VLAN setting.</td>
</tr>
<tr>
<td>5</td>
<td>Press <strong>Validate</strong>.</td>
</tr>
<tr>
<td>6</td>
<td>Press <strong>Save</strong>.</td>
</tr>
</tbody>
</table>

Set SW Port Configuration Field

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Unlock network configuration options.</td>
</tr>
<tr>
<td>2</td>
<td>Scroll to the SW Port Configuration option and then press <strong>Edit</strong>.</td>
</tr>
<tr>
<td>3</td>
<td>Scroll to the setting that you want and then press <strong>Select</strong>.</td>
</tr>
<tr>
<td>4</td>
<td>Press <strong>Save</strong>.</td>
</tr>
</tbody>
</table>

Set PC Port Configuration Field

To configure the setting on multiple phones simultaneously, enable Remote Port Configuration in Enterprise Phone Configuration (**System > Enterprise Phone Configuration**).

**Note**

If the ports are configured for Remote Port Configuration in Cisco Unified Communications Manager, the data cannot be changed on the phone.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Unlock network configuration options.</td>
</tr>
<tr>
<td>2</td>
<td>Scroll to the PC Port Configuration option and then press <strong>Edit</strong>.</td>
</tr>
<tr>
<td>3</td>
<td>Scroll to the setting that you want and then press <strong>Select</strong>.</td>
</tr>
<tr>
<td>4</td>
<td>Press <strong>Save</strong>.</td>
</tr>
</tbody>
</table>
Set PC VLAN Field

Procedure

Step 1 Unlock network configuration options.
Step 2 Make sure the Admin VLAN ID option is set.
Step 3 Scroll to the PC VLAN option.
Step 4 Press Edit.
Step 5 Enter a new PC VLAN setting.
Step 6 Press Validate.
Step 7 Press Save.

Set DHCP Field

Procedure

Step 1 Unlock network configuration options.
Step 2 Scroll to the DHCP option and press No to disable DHCP, or press Yes to enable DHCP.
Step 3 Press Save.

Set IP Address Field

Procedure

Step 1 Unlock network configuration options.
Step 2 Set the DHCP option to No.
Step 3 Scroll to the IP Address option, press Edit and enter a new IP Address.
Step 4 Press Validate and Save.
Set Subnet Mask Field

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Unlock network configuration options.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Set the DHCP option to <strong>No</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Scroll to the Subnet Mask option, press <strong>Edit</strong>, and then enter a new subnet mask.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Press <strong>Validate</strong> and then press <strong>Save</strong>.</td>
</tr>
</tbody>
</table>

Set Default Router Fields

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Unlock network configuration options.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Set the DHCP option to <strong>No</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Scroll to the appropriate Default Router option, press <strong>Edit</strong>, and then enter a new router IP address.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Press <strong>Validate</strong>.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Repeat Steps 3 and 4 as needed to assign backup routers.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Press <strong>Save</strong>.</td>
</tr>
</tbody>
</table>

Set DNS Server Fields

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Unlock network configuration options.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Set the DHCP option to <strong>No</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Scroll to the appropriate DNS Server option, press <strong>Edit</strong>, and then enter a new DNS server IP address.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Press <strong>Validate</strong>.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Repeat Steps 3 and 4 as needed to assign backup DNS servers.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Press <strong>Save</strong>.</td>
</tr>
</tbody>
</table>
Set DHCP Address Released Field

Procedure

Step 1 Unlock network configuration options.
Step 2 Scroll to the DHCP Address Released option and press Yes to release the IP address assigned by DHCP, or press No if you do not want to release this IP address.
Step 3 Press Save.

Set Alternate TFTP Field

Procedure

Step 1 Unlock network configuration options.
Step 2 Scroll to the Alternate TFTP option and press Yes if the phone should use an alternative TFTP server.
Step 3 Press Save.

Set TFTP Server 1 Field

Procedure

Step 1 Unlock the CTL or ITL file if necessary (for example, if you are changing the administrative domain of the phone). If both the CTL and ITL files exist, unlock either of the files.
Step 2 If DHCP is enabled, set the Alternate TFTP option to Yes.
Step 3 Scroll to the TFTP Server 1 option, press Edit, and then enter a new TFTP server IP address.
Step 4 Press Validate, and then press Save.
Set TFTP Server 2 Field

**Note**
If you forgot to unlock the CTL or ITL file, you can change the TFTP Server 2 address in either file, then erase them by pressing **Erase** from the Security Configuration menu. A new CTL or ITL file downloads from the new TFTP Server 2 address.

**Procedure**

**Step 1** Unlock the CTL or ITL file if necessary (for example, if you are changing the administrative domain of the phone). If both the CTL and ITL files exist, unlock either of the files.

**Step 2** Unlock network configuration options.

**Step 3** Enter an IP address for the TFTP Server 1 option.

**Step 4** Scroll to the TFTP Server 2 option, press **Edit**, and then enter a new backup TFTP server IP address.

**Step 5** Press **Validate**, and then press **Save**.

---

Set DHCPv6 Field

**Procedure**

**Step 1** Unlock network configuration options.

**Step 2** Scroll to the DHCPv6 option and press **No** to disable DHCP, or press **Yes** to enable DHCP.

**Step 3** Press **Save**.

---

Set IPv6 Address Field

**Procedure**

**Step 1** Unlock network configuration options.

**Step 2** Set the DHCPv6 option to **No**.

**Step 3** Scroll to the IP Address option, press **Edit**, and then enter a new IP Address.

**Step 4** Press **Validate** and then press **Save**.
Set IPv6 Prefix Length Field

Procedure

Step 1  Unlock network configuration options.
Step 2  Set the DHCPv6 option to No.
Step 3  Scroll to the IPv6 Prefix Length option, press Edit, and then enter a new subnet mask.
Step 4  Press Validate and then press Save.

Set IPv6 Default Router 1 Field

Procedure

Step 1  Unlock network configuration options.
Step 2  Set the DHCPv6 option to No.
Step 3  Scroll to the appropriate Default Router option, press the Edit softkey, and then enter a new router IP address.
Step 4  Press the Validate softkey.
Step 5  Repeat Steps 3 and 4 as needed to assign the backup router.
Step 6  Press the Save softkey.

Set IPv6 DNS Server 1 and IPv6 DNS Server 2 Fields

Procedure

Step 1  Unlock network configuration options.
Step 2  Set the DHCPv6 option to No.
Step 3  Scroll to the appropriate DNS Server option, press Edit, and then enter a new DNS server IP address.
Step 4  Press Validate.
Step 5  Repeat Steps 3 and 4 as needed to assign the backup DNS server.
Step 6  Press Save.
Set DHCPv6 Address Released Field

Procedure

**Step 1** Unlock network configuration options.
**Step 2** Scroll to the DHCPv6 Address Released option and press **Yes** to release the IP address assigned by DHCP, or press **No** if you do not want to release this IP address.
**Step 3** Press **Save**.

Set IPv6 Alternate TFTP Field

Procedure

**Step 1** Unlock network configuration options.
**Step 2** Scroll to the IPv6 Alternate TFTP option and press **Yes** if the phone should use an alternative TFTP server.
**Step 3** Press **Save**.

Set IPv6 TFTP Server 1 Field

Procedure

**Step 1** Unlock the CTL or ITL file if necessary. If both the CTL and ITL files exist, unlock either of the files.
**Step 2** If DHCPv6 is enabled, set the Alternate TFTP option to **Yes**.
**Step 3** Scroll to the IPv6 TFTP Server 1 option, press **Edit**, and then enter a new TFTP server IP address.
**Step 4** Press **Validate**, and then press **Save**.
Set IPv6 TFTP Server 2 Field

**Procedure**

1. Unlock the CTL or ITL file if necessary. If both the CTL and ITL files exist, unlock either of the files.
2. Unlock network configuration options.
3. Enter an IP address for the IPv6 TFTP Server 1 option.
4. Scroll to the IPv6 TFTP Server 2 option, press **Edit**, and then enter a new backup TFTP server IP address.
5. Press **Validate**, and then press **Save**.

**DHCPv6 and Autoconfiguration**

You can configure the IP address and other network settings (such as the TFTP server, DNS server, domain, name) on an IP phone manually or by using a router or a DHCP server to automatically assign the IP address and other network information. For more information on how the Allow Auto Configuration for Phones and DHCPv6 settings determine where the IP phone acquires the IPv6 address and other network settings, see the following table.

**Table 14: Determine where a Phone Acquires its Network Settings**

<table>
<thead>
<tr>
<th>DHCPv6</th>
<th>Auto IP configuration</th>
<th>How the phone acquires its IP address and network settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
<td>Disabled</td>
<td>You must manually configure an IP address and the other network settings.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> When DHCPv6 is disabled, the Auto IP Configuration setting is ignored.</td>
</tr>
<tr>
<td>Disabled</td>
<td>Enabled</td>
<td>You must manually configure an IP address and the other network settings.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> When DHCPv6 is disabled, the Auto IP Configuration setting is ignored.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Disabled</td>
<td>The DHCP server assigns the IP address and the other network settings to the phone.</td>
</tr>
</tbody>
</table>
How the phone acquires its IP address and network settings

<table>
<thead>
<tr>
<th>DHCPv6</th>
<th>Auto IP configuration</th>
<th>How the phone acquires its IP address and network settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Enabled</td>
<td>When the M-bit is set on the router, the O-bit is ignored. The phone can set the IPv6 address based on an IPv6 address that it received from a DHCPv6 server or the phone can acquire the IPv6 address through stateless address autoconfiguration. When the M-bit is not set, you should set the O-bit on the router. The phone will then acquire the IPv6 address through stateless address autoconfiguration. The phone will not request an IPv6 address from the DHCPv6 server, but it will request other network configuration information.</td>
</tr>
</tbody>
</table>

Related Topics
Display Settings Menu, on page 62
Unlock and Lock Options, on page 63
Value Input Guidelines, on page 63
Phone Setup Options, on page 64
Device Configuration Menu, on page 85

Device Configuration Menu

The Device Configuration menu provides access to nine submenus from which you can view a variety of settings that are specified in the configuration file for a phone. The phone downloads the configuration file from the TFTP server. These submenus are:

For instructions about how to access the Device Configuration menu and its submenus, see Display Settings Menu, on page 62.

Unified CM Configuration Menu

The Unified CM Configuration menu contains the options Unified CM1, Unified CM2, Unified CM3, Unified CM4, and Unified CM5. These options show the Cisco Unified Communications Manager servers that are available to process from the phone, in prioritized order. To change these options, use Cisco Unified Communications Manager Administration, Cisco Unified CM Group Configuration.

For an available Cisco Unified Communications Manager server, an option on the Unified CM Configuration menu will show the Cisco Unified Communications Manager server IP address or name and one of the states shown in the following table.
Table 15: Cisco Unified Communications Manager Server States

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Cisco Unified Communications Manager server from which the phone is currently receiving call-processing services</td>
</tr>
<tr>
<td>Standby</td>
<td>Cisco Unified Communications Manager server to which the phone switches if the current server becomes unavailable</td>
</tr>
<tr>
<td>Blank</td>
<td>No current connection to this Cisco Unified Communications Manager server</td>
</tr>
</tbody>
</table>

An option may also display one of more of the designations or icons shown in the following table.

Table 16: Cisco Unified Communications Manager Server Designations

<table>
<thead>
<tr>
<th>Designation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRST</td>
<td>Indicates a Survivable Remote Site Telephony router that can provide Cisco Unified Communications Manager functionality with a limited feature set. This router assumes control of call processing if all other Cisco Unified Communications Manager servers become unreachable. The SRST Cisco Unified Communications Manager always appears last in the list of servers, even if it is active. For more information, see the “Survivable Remote Site Telephony Configuration” chapter in the Cisco Unified Communications Manager Administration Guide.</td>
</tr>
<tr>
<td>TFTP</td>
<td>Indicates that the phone was unable to register with a Cisco Unified Communications Manager listed in its configuration file, and it registered with the TFTP server instead.</td>
</tr>
<tr>
<td>![Authentication icon]</td>
<td>Appears as a shield and indicates that the call is from a trusted device, and that the connection to Cisco Unified Communications Manager is authenticated. For more information about authentication, see the Cisco Unified Communications Manager Security Guide.</td>
</tr>
<tr>
<td>![Encryption icon]</td>
<td>Appears as a padlock and indicates that the call is from a trusted device, and that the connection to Cisco Unified Communications Manager is authenticated and encrypted. For more information about authentication and encryption, see the Cisco Unified Communications Manager Security Guide. The Encryption icon is also displayed when a Cisco Unified IP Phone is configured as protected. For more information about protected calls, see the Cisco Unified Communications Manager Security Guide. Protected calls are not authenticated.</td>
</tr>
</tbody>
</table>
SIP Configuration Menu for SIP Phones

The SIP Configuration menu is available on SIP phones. This menu contains these submenus:

SIP General Configuration Menu

The SIP General Configuration menu displays information about the configurable SIP parameters on a SIP phone. The following table describes the options in this menu.

Table 17: SIP General Configuration Menu Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preferred CODEC</td>
<td>Displays the CODEC to use when a call is initiated. This value will always be set to none.</td>
<td>Display only. Cannot configure.</td>
</tr>
<tr>
<td>Out of Band DTMF</td>
<td>Displays the configuration of the out-of-band signaling (for tone detection on the IP side of a gateway). The Cisco Unified IP Phone (SIP) uses the AVT tone method to support out of band signaling. This value will always be set to avt.</td>
<td>Display only. Cannot configure.</td>
</tr>
<tr>
<td>Register with Proxy</td>
<td>This value will always be set to Yes.</td>
<td>Display only. Cannot configure.</td>
</tr>
<tr>
<td>Register Expires</td>
<td>Displays the amount of time, in seconds, after which a registration request expires.</td>
<td>From Cisco Unified Communications Manager Administration, choose Device &gt; Device Settings &gt; SIP Profile.</td>
</tr>
<tr>
<td>Phone Label</td>
<td>Displays the text that is displayed on the top right status line of the LCD on the phone. This text is for end-user display only and has no effect on caller identification or messaging. This value will always be set to null.</td>
<td>Display only. Cannot configure.</td>
</tr>
<tr>
<td>Enable VAD</td>
<td>This value is set to No by default.</td>
<td>From Cisco Unified Communications Manager Administration, choose Device &gt; Device Settings &gt; SIP Profile.</td>
</tr>
<tr>
<td>Start Media Port</td>
<td>Displays the start Real-Time Transport Protocol (RTP) range for media.</td>
<td>From Cisco Unified Communications Manager Administration, choose Device &gt; Device Settings &gt; SIP Profile.</td>
</tr>
</tbody>
</table>
To Change Description Option from CiscoUnifiedCommunications Manager Administration, choose Device > Device Settings > SIP Profile.

Displaysthe end Real-Time Transport Protocol (RTP) range formedia.

**End Media Port**

Displays if Network Address Translation (NAT) is enabled. This value will always be set to false.

**NAT Enabled**

Displays the WAN IP address of the NAT or firewall server. This value will always be set to null.

**NAT Address**

This value is set to No by default.

**Call Statistics**

Related Topics

- Display Settings Menu, on page 62
- Device Configuration Menu, on page 85

### Line Settings Menu for SIP Phones

The Line Settings menu displays information that relates to the configurable parameters for each of the lines on a SIP phone. The following table describes the options in this menu.

**Table 18: Line Settings Menu Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Displays the lines and the number used to register each line.</td>
<td>Use Cisco Unified Communications Manager Administration to modify.</td>
</tr>
<tr>
<td><strong>Short Name</strong></td>
<td>Displays the short name configured for the line.</td>
<td>Use Cisco Unified Communications Manager Administration to modify.</td>
</tr>
</tbody>
</table>
To change Description Option
Use Cisco Unified Communications Manager Administration to modify.

Display the name used by the phone for authentication if a registration is challenged by the call control server during initialization.
The length of the SIP digest authentication name has been increased to 128 characters for Cisco Unified 7900 Series SIP phones. The authentication name is used to verify that the phone is allowed to send SIP messages (REGISTER, INVITE, and SUBSCRIBE) to Cisco Unified Communications Manager.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Longer Authentication Name</td>
<td>Displays the name used by the phone for authentication if a registration is challenged by the call control server during initialization. The length of the SIP digest authentication name has been increased to 128 characters for Cisco Unified 7900 Series SIP phones. The authentication name is used to verify that the phone is allowed to send SIP messages (REGISTER, INVITE, and SUBSCRIBE) to Cisco Unified Communications Manager.</td>
<td>Use Cisco Unified Communications Manager Administration to modify.</td>
</tr>
<tr>
<td>Display Name</td>
<td>Displays the identification the phone uses for display for caller identification purposes.</td>
<td>Use Cisco Unified Communications Manager Administration to modify.</td>
</tr>
<tr>
<td>Proxy Address</td>
<td>The value is left blank because it does not apply to SIP phones that are using Cisco Unified Communications Manager.</td>
<td>Display only. Cannot configure.</td>
</tr>
<tr>
<td>Proxy Port</td>
<td>The value is left blank because it does not apply to SIP phones that are using Cisco Unified Communications Manager.</td>
<td>Display only. Cannot configure.</td>
</tr>
<tr>
<td>Shared Line</td>
<td>Displays if the line is part of a shared line (Yes) or not (No).</td>
<td>Display only. Cannot configure.</td>
</tr>
</tbody>
</table>

Related Topics
Display Settings Menu, on page 62
Device Configuration Menu, on page 85

Call Preferences Menu for SIP Phones

The Call Preferences menu displays settings that relate to the settings for the call preferences on a SIP phone. The following table describes the options in this menu.
Table 19: Call Preferences Menu Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Caller ID Blocking</td>
<td>Indicates whether caller ID blocking is enabled (Yes) or disabled (No) for the phone.</td>
<td>From Cisco Unified Communications Manager Administration, choose <strong>Device</strong> &gt; <strong>Device Settings</strong> &gt; <strong>SIP Profile</strong>.</td>
</tr>
<tr>
<td>Anonymous Call Block</td>
<td>Indicates whether anonymous call block is enabled (Yes) or disabled (No) for the phone.</td>
<td>From Cisco Unified Communications Manager Administration, choose <strong>Device</strong> &gt; <strong>Device Settings</strong> &gt; <strong>SIP Profile</strong>.</td>
</tr>
<tr>
<td>Call Waiting Preferences</td>
<td>Displays a sub-menu that indicates whether call waiting is enabled (Yes) or disabled (No) for each line.</td>
<td>From Cisco Unified Communications Manager Administration, choose <strong>Call Routing</strong> &gt; <strong>Directory Number</strong>.</td>
</tr>
<tr>
<td>Call Hold Ringback</td>
<td>Indicates whether the call hold ringback feature is enabled (Yes) or disabled (No) for the phone.</td>
<td>From Cisco Unified Communications Manager Administration, choose <strong>Device</strong> &gt; <strong>Device Settings</strong> &gt; <strong>SIP Profile</strong>.</td>
</tr>
<tr>
<td>Stutter Msg Waiting</td>
<td>Indicates whether stutter message waiting is enabled (Yes) or disabled (No) for the phone.</td>
<td>From Cisco Unified Communications Manager Administration, choose <strong>Device</strong> &gt; <strong>Device Settings</strong> &gt; <strong>SIP Profile</strong>.</td>
</tr>
<tr>
<td>Call Logs BLF Enabled</td>
<td>Indicates whether BLF for call logs is enabled (Yes) or disabled (No) for the phone.</td>
<td>Use Cisco Unified Communications Manager Administration.</td>
</tr>
<tr>
<td>Auto Answer Preferences</td>
<td>Displays a sub-menu that indicates whether auto answer is enabled (Yes) or disabled (No) for the each line.</td>
<td>From Cisco Unified Communications Manager Administration, choose <strong>Call Routing</strong> &gt; <strong>Directory Number</strong>.</td>
</tr>
<tr>
<td>Speed Dials</td>
<td>Displays a sub-menu that displays the lines available on the phone. Select a line to see the speed dial label and number assigned to that line.</td>
<td>From Cisco Unified Communications Manager Administration, choose <strong>Device</strong> &gt; <strong>Add a New Speed Dial</strong>.</td>
</tr>
</tbody>
</table>

**Related Topics**

- Display Settings Menu, on page 62
- Device Configuration Menu, on page 85

**HTTP Configuration Menu**

The HTTP Configuration menu displays the URLs of servers from which the phone obtains a variety of information. This menu also displays information about the idle display on the phone.
Cisco Unified IP Phones do not support URLs with IPv6 addresses in the URL. This includes hostname which maps to an IPv6 address for directories, services, messages, and information URLs. If you support phone use of URLs, you must configure the phone and the servers that provide URL services with IPv4 addresses.

The following table describes the HTTP Configuration menu options.

**Table 20: HTTP Configuration Menu Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directories URL</td>
<td>URL of the server from which the phone obtains directory information.</td>
<td>From Cisco Unified Communications Manager Administration, choose Device &gt; Phone &gt; Phone Configuration.</td>
</tr>
<tr>
<td>Services URL</td>
<td>URL of the server from which the phone obtains Cisco Unified IP Phone services.</td>
<td>From Cisco Unified Communications Manager Administration, choose Device &gt; Phone &gt; Phone Configuration.</td>
</tr>
<tr>
<td>Messages URL</td>
<td>URL of the server from which the phone obtains message services.</td>
<td>From Cisco Unified Communications Manager Administration, choose Device &gt; Phone &gt; Phone Configuration.</td>
</tr>
<tr>
<td>Information URL</td>
<td>URL of the help text that appears on the phone.</td>
<td>From Cisco Unified Communications Manager Administration, choose Device &gt; Phone &gt; Phone Configuration.</td>
</tr>
<tr>
<td>Authentication URL</td>
<td>URL that the phone uses to validate requests made to the phone web server.</td>
<td>From Cisco Unified Communications Manager Administration, choose Device &gt; Phone &gt; Phone Configuration.</td>
</tr>
<tr>
<td>Proxy Server URL</td>
<td>URL of proxy server, which makes HTTP requests to remote host addresses on behalf of the phone HTTP client and provides responses from the remote host to the phone HTTP client.</td>
<td>From Cisco Unified Communications Manager Administration, choose Device &gt; Phone &gt; Phone Configuration.</td>
</tr>
</tbody>
</table>
Idle URL | URL of an XML service that the phone displays when the phone has not been used for the time specified in the Idle URL Time option and no menu is open. For example, you could use the Idle URL option and the Idle URL Time option to display a stock quote or a calendar on the LCD screen when the phone has not been used for 5 minutes. | From Cisco Unified Communications Manager Administration, choose Device > Phone > Phone Configuration.

Idle URL Time | Number of seconds that the phone has not been used and no menu is open before the XML service specified in the Idle URL option is activated. | From Cisco Unified Communications Manager Administration, choose Device > Phone > Phone Configuration.

---

**Locale Configuration Menu**

The Locale Configuration menu displays information about the user locale and the network locale used by the phone. The following table describes the options on this menu.

**Table 21: Locale Configuration Menu Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Locale</td>
<td>User locale associated with the phone user. The user locale identifies a set of detailed information to support users, including language, font, date and time formatting, and alphanumeric keyboard text information. For more information on user locale installation, see the Cisco Unified Communications Operating System Administration Guide.</td>
<td>From Cisco Unified Communications Manager Administration, choose Device &gt; Phone &gt; Phone Configuration.</td>
</tr>
<tr>
<td>User Locale Version</td>
<td>Version of the user locale loaded on the phone.</td>
<td>Display only. Cannot configure.</td>
</tr>
<tr>
<td>User Locale CharSet</td>
<td>Character set that the phone uses for the user locale.</td>
<td>Display only. Cannot configure.</td>
</tr>
</tbody>
</table>
To change Description Option
From Cisco Unified Communications Manager Administration, choose Device > Phone > Phone Configuration.

Network Locale
Network locale associated with the phone user. The network locale identifies a set of detailed information that supports the phone in a specific location, including definitions of the tones and cadences used by the phone.

Network Locale Version
Version of the network locale loaded on the phone.

NTP Configuration (SIP phones only)
Provides access to the NTP Configuration Menu. For more information, see NTP Configuration Menu for SIP Phones, on page 93.

NTP Configuration Menu for SIP Phones
The NTP Configuration menu displays information about the NTP server and mode configuration used by SIP phones. The following table describes the options on this menu.

Table 22: NTP Configuration Menu Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTP IP Address 1</td>
<td>IP address of the primary NTP server.</td>
<td>From Cisco Unified Communications Manager Administration, choose System &gt; Phone &gt; NTP Reference.</td>
</tr>
<tr>
<td>NTP IP Address 2</td>
<td>IP address of the secondary or backup NTP server.</td>
<td>From Cisco Unified Communications Manager Administration, choose System &gt; Phone &gt; NTP Reference.</td>
</tr>
<tr>
<td>NTP Mode 1</td>
<td>Primary server mode. Supported modes are Directed Broadcast and Unicast.</td>
<td>From Cisco Unified Communications Manager Administration, choose System &gt; Phone &gt; NTP Reference.</td>
</tr>
<tr>
<td>NTP Mode 2</td>
<td>Secondary server mode. Supported modes are Directed Broadcast and Unicast.</td>
<td>From Cisco Unified Communications Manager Administration, choose System &gt; Phone &gt; NTP Reference.</td>
</tr>
</tbody>
</table>

UI Configuration Menu
The UI Configuration menu displays the status of various user interface features on the phone. The following table describes the options on this menu.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto Line Select</td>
<td>Indicates whether the phone shifts the call focus to incoming calls on all lines. When this option is disabled, the phone only shifts the call focus to incoming calls on the line that is in use. When this option is enabled, the phone shifts the call focus to the line with the most recent incoming call. Default: Disabled.</td>
<td>From Cisco Unified Communications Manager Administration, choose Device &gt; Phone &gt; Phone Configuration.</td>
</tr>
<tr>
<td>BLF for Call Lists</td>
<td>Indicates whether the Busy Lamp Field (BLF) is enabled for call lists.</td>
<td>From Cisco Unified Communications Manager Administration, choose System &gt; Enterprise Parameters.</td>
</tr>
<tr>
<td>Reverting Focus Priority</td>
<td>Indicates whether the phone shifts the call focus on the phone screen to an incoming call or a reverting hold call. Settings include: Lower: Focus priority given to incoming calls. Higher: Focus priority given to reverting calls. Even: Focus priority given to the first call.</td>
<td>From Cisco Unified Communications Manager Administration, choose System &gt; Device Pool. See also: Hold Reversion.</td>
</tr>
<tr>
<td>Auto Call Select</td>
<td>Indicates whether the phone automatically shifts the call focus to an incoming call on the same line when the user is already on a call. When this option is enabled, the phone shifts the call focus to the most recent incoming call. When this option is disabled, all automatic focus changes, including Auto Line Select, are disabled regardless of their setting. Default: Enabled.</td>
<td>From Cisco Unified Communications Manager Administration, choose Device &gt; Phone &gt; Phone Configuration.</td>
</tr>
<tr>
<td>“more” Softkey Timer</td>
<td>Indicates the number of seconds that additional softkeys display after the user presses more. If this timer expires before the user presses another softkey, the display reverts to the initial softkeys. Range: 5 to 30; 0 represents an infinite timer. Default: 5</td>
<td>From Cisco Unified Communications Manager Administration, choose Device &gt; Phone &gt; Phone Configuration.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>To change</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Wideband Headset</td>
<td>Indicates whether the user can configure the Wideband Headset option in the</td>
<td>From Cisco Unified Communications Manager Administration, choose Device &gt;</td>
</tr>
<tr>
<td></td>
<td>Wideband Headset option in the phone user interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Values:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enabled: The user can configure the Wideband Headset option in the Audio</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Preferences menu on the phone (choose User Preferences &gt; Audio Preferences &gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Wideband Headset).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Disabled: The value of the Wideband Headset option in Cisco Unified</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Communications Manager Administration gets used (see Media Configuration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Menu, on page 96).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Default: Enabled</td>
<td></td>
</tr>
<tr>
<td>Wideband Handset</td>
<td>Indicates whether the user can configure the Wideband Handset option in the</td>
<td>From Cisco Unified Communications Manager Administration, choose Device &gt;</td>
</tr>
<tr>
<td></td>
<td>Wideband Handset option in the phone user interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Values:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enabled: The user can configure the Wideband Handset option in the Audio</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Preferences menu on the phone (choose User Preferences &gt; Audio Preferences &gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Wideband Handset).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Disabled: The value of the Wideband Handset option in Cisco Unified</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Communications Manager Administration gets used (see Media Configuration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Menu, on page 96).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Default: Enabled</td>
<td></td>
</tr>
<tr>
<td>Personalization</td>
<td>Indicates whether the phone has been enabled for configuration of custom</td>
<td>From Cisco Unified Communications Manager Administration, choose Device &gt;</td>
</tr>
<tr>
<td></td>
<td>ring tones and wallpaper images.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Default: Enabled</td>
<td></td>
</tr>
<tr>
<td>Single Button Barge</td>
<td>Indicates whether the Single Button Barge feature is enabled for the phone.</td>
<td>From Cisco Unified Communications Manager Administration, choose Device &gt;</td>
</tr>
</tbody>
</table>
### Media Configuration Menu

The Media Configuration menu displays whether the headset, speakerphone, and video capability (SCCP phones only) are enabled on the phone. This menu also displays options for recording tones that the phone may play to indicate that a call may be recorded. The following table describes the options on this menu.

**Table 24: Media Configuration Menu Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enbloc Dialing (SCCP only)</td>
<td>Indicates whether the phone will use Enbloc dialing. If “Enabled”, the phone uses Enbloc dialing when possible. If “Disabled”, the phone does not use Enbloc dialing. You should disable Enbloc dialing if either Forced Authorization Codes (FAC) or Client Matter Codes (CMC) dialing is in use. <strong>Default:</strong> Enabled</td>
<td>From Cisco Unified Communications Manager Administration, choose Device &gt; Phone &gt; Phone Configuration.</td>
</tr>
<tr>
<td>Headset Enabled</td>
<td>Indicates whether the Headset button is enabled on the phone.</td>
<td>From Cisco Unified Communications Manager Administration, choose Device &gt; Phone &gt; Phone Configuration.</td>
</tr>
<tr>
<td>Headset Hookswitch Control Enabled (for Cisco Unified IP Phone 7975G, 7965G, and 7945G)</td>
<td>Indicates whether the wireless headset hookswitch feature is enabled on the phone.</td>
<td>From Cisco Unified Communications Manager Administration, choose Device &gt; Phone &gt; Phone Configuration.</td>
</tr>
<tr>
<td>Speaker Enabled</td>
<td>Indicates whether the speakerphone is enabled on the phone.</td>
<td>From Cisco Unified Communications Manager Administration, choose Device &gt; Phone &gt; Phone Configuration.</td>
</tr>
<tr>
<td>Video Capability Enabled (SCCP phones only)</td>
<td>Indicates whether the phone can participate in video calls when connected to an appropriately equipped computer.</td>
<td>From Cisco Unified Communications Manager Administration, choose Device &gt; Phone &gt; Phone Configuration.</td>
</tr>
</tbody>
</table>
To change Description Option
From Cisco Unified Communications Manager Administration, choose Device > Phone > Phone Configuration.

### Recording Tone
Indicates whether a recording tone (often referred to as a beep tone) is enabled or disabled for the phone. If the recording tone option is enabled, the phone plays the beep tone in both directions of every call, regardless of whether the call actually gets recorded. The beep tone first sounds when a call is answered.

You may want to notify your users if you enable this option.

Default: Disabled

Related Parameters:
- Recording Tone Local Volume
- Recording Tone Remote Volume
- Recording Tone Duration

Other related parameters—Beep tone frequency in Hz, the length of the beep tone (called duration), and how often the beep tone plays (called interval)—are defined on a per-Network Locale basis in the xml file that defines tones. This xml file is usually named tones.xml or g3-tones.xml.

### Recording Tone Local Volume
Indicates the loudness setting for the beep tone that is received by the party whose phone has the Recording Tone option enabled.

This setting applies for each listening device (handset, speakerphone, headset).

Range: 0 percent (no tone) to 100 percent (same level as current volume setting on the phone).

Default: 100

See also Recording Tone in this table.

From Cisco Unified Communications Manager Administration, choose Device > Phone > Phone Configuration.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recording Tone Remote Volume</td>
<td>Indicates the loudness setting for the beep tone that the remote party receives. The remote party is the party who is on a call with the party whose phone has the Recording Tone option enabled. Range: 0 percent to 100 percent. (0 percent is ~66 dBM and 100 percent is ~3 dBM.) Default: 84 percent (~10 dBM) See also Recording Tone in this table.</td>
<td>From Cisco Unified Communications Manager Administration, choose Device &gt; Phone &gt; Phone Configuration.</td>
</tr>
<tr>
<td>Recording Tone Duration</td>
<td>Indicates the length of time in milliseconds that the beep tone plays. If the value you configure here is less than one third the interval, then this value overrides the default provided by the Network Locale. Range: 0 to 3000. Note For some Network Locales that use a complex cadence, this setting applies only to the first beep tone. See also Recording Tone in this table.</td>
<td>From Cisco Unified Communications Manager Administration, choose Device &gt; Phone &gt; Phone Configuration.</td>
</tr>
<tr>
<td>Wideband Headset</td>
<td>Indicates whether wideband is enabled or disabled for the headset. Default: Disabled</td>
<td>If Wideband Headset UI Control is enabled, you or the user can use the phone and choose User Preferences &gt; Audio Preferences &gt; Wideband Headset. If Wideband Headset UI Control is disabled, from Cisco Unified Communications Manager Administration choose Device &gt; Phone &gt; Phone Configuration to set this value. Note If you allowed this option to be user controllable (in the Wideband Headset UI Control option), the user-configured value takes precedence.</td>
</tr>
</tbody>
</table>
To change Description Option

If Wideband Handset UI Control is enabled, you or the user can choose
<User Preferences > Audio Preferences > Wideband Handset.

If Wideband Handset UI Control is disabled, use Cisco Unified Communications Manager administration and choose Device > Phone > Phone Configuration to set this value.

Note: If you allowed this option to be user controllable (in the Wideband Handset UI Control option), the user-configured value takes precedence.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wideband Handset</td>
<td>Indicates whether wideband is enabled or disabled for the handset.</td>
<td>If Wideband Handset UI Control is enabled, you or the user can choose</td>
</tr>
<tr>
<td></td>
<td>Default: “Use Phone Default” on Cisco Unified Communications Manager Administration. (This default means that the phone will be enabled for a wideband handset only if the phone was shipped with a wideband handset.)</td>
<td>Cisco Unified Communications Manager Administration &gt; User Preferences &gt; Audio Preferences &gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Wideband Handset.</td>
</tr>
<tr>
<td>Enterprise Advertise G.722 Codec</td>
<td>Enables/disables (enabled by default) Cisco Unified IP Phones to advertise the G.722 codec to Cisco Unified Communications Manager. For more information, see the Cisco Unified Communications Manager System Guide, “Cisco Unified IP Phones” chapter, “Codec Usage” section.</td>
<td>From Cisco Unified Communications Manager Administration, choose System &gt; Enterprise Parameters.</td>
</tr>
<tr>
<td></td>
<td>Note: When a phone is registered with a Cisco Unified Communications Manager that does not support this setting, the default is “Disabled.”</td>
<td></td>
</tr>
<tr>
<td>Device Advertise G.722 Codec</td>
<td>Allows you to override the Enterprise Advertise G.722 Codec on a per-phone basis. The default is “Use System Default,” which means the value configured for the Enterprise Advertise G.722 Codec parameter gets used.</td>
<td>From Cisco Unified Communications Manager Administration, choose Device &gt; Phone.</td>
</tr>
</tbody>
</table>

**Power Save Configuration Menu**

The Power Save Configuration menu displays the settings that control the LCD phone screen turning off to conserve power. The following table describes the options on this menu.

For detailed information about these settings, see EnergyWise Setup on Cisco Unified IP Phone, on page 159.
Table 25: Power Save Configuration Menu Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display On Time</td>
<td>Time each day that the LCD screen turns on automatically (except on the days specified in the Days Display Not Active field).</td>
<td>From Cisco Unified Communications Manager Administration, choose <strong>Device &gt; Phone &gt; Phone Configuration</strong>.</td>
</tr>
<tr>
<td>Display On Duration</td>
<td>Length of time that the LCD screen remains on after it turns on at the time shown in the Display On Time option.</td>
<td>From Cisco Unified Communications Manager Administration, choose <strong>Device &gt; Phone &gt; Phone Configuration</strong>.</td>
</tr>
<tr>
<td>Display Idle Timeout</td>
<td>Length of time that the phone is idle before the display turns off. Applies only when the display was off as scheduled and the end user turned it on (by pressing a button on the phone, touching the touchscreen, or lifting the handset).</td>
<td>From Cisco Unified Communications Manager Administration, choose <strong>Device &gt; Phone &gt; Phone Configuration</strong>.</td>
</tr>
<tr>
<td>Days Display Not Active</td>
<td>Days that the display does not turn on automatically at the time specified in the Display On Time option.</td>
<td>From Cisco Unified Communications Manager Administration, choose <strong>Device &gt; Phone &gt; Phone Configuration</strong>.</td>
</tr>
<tr>
<td>Display On When Incoming Call</td>
<td>Indicates whether the LCD screen automatically illuminates when a call is received.</td>
<td>From Cisco Unified Communications Manager Administration, choose <strong>Device &gt; Phone &gt; Phone Configuration</strong>.</td>
</tr>
</tbody>
</table>

**Ethernet Configuration Menu**

The Ethernet Configuration menu includes the options that are described in the following table.
Table 26: Ethernet Configuration Menu Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forwarding Delay</td>
<td>Indicates whether the internal switch begins to forward packets between the PC port and switched port on the phone when the phone becomes active.</td>
<td>From Cisco Unified Communications Manager Administration, choose Device &gt; Phone &gt; Phone Configuration.</td>
</tr>
<tr>
<td></td>
<td>• When Forwarding Delay is set to disabled, the internal switch begins to forward packets immediately.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• When Forwarding Delay is set to enabled, the internal switch waits 8 seconds before it begins to forward packets between the PC port and the switch port.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Default is disabled.</td>
<td></td>
</tr>
<tr>
<td>Span to PC Port</td>
<td>Indicates whether the phone will forward packets transmitted and received on the network port to the access port.</td>
<td>From Cisco Unified Communications Manager Administration, choose Device &gt; Phone &gt; Phone Configuration.</td>
</tr>
<tr>
<td></td>
<td>Enable this option if an application that requires phone traffic monitoring is running on the access port. These applications include monitoring and recording applications (common in call center environments) and network packet capture tools that are used for diagnostic purposes.</td>
<td></td>
</tr>
</tbody>
</table>

Security Configuration Menu

The Security Configuration menu that you display from the Device Configuration menu displays settings that relate to security for the phone.

Note

The phone also has a Security Configuration menu that you access directly from the Settings menu. For information about the security options on that menu, see Security Configuration Menu, on page 109.

The following table describes the options on the Security Configuration menu.
Table 27: Security Configuration Menu Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC Port Disabled</td>
<td>Indicates whether the access port on the phone is enabled or disabled.</td>
<td>From Cisco Unified Communications Manager Administration, choose Device &gt; Phone &gt; Phone Configuration.</td>
</tr>
<tr>
<td></td>
<td><em>Note</em> If disabled, video will not work on this phone, even if video is enabled.</td>
<td></td>
</tr>
<tr>
<td>GARP Enabled</td>
<td>Indicates if the phone accepts MAC addresses from Gratuitous ARP responses.</td>
<td>From Cisco Unified Communications Manager Administration, choose Device &gt; Phone &gt; Phone Configuration.</td>
</tr>
<tr>
<td>Voice VLAN Enabled</td>
<td>Indicates whether the phone allows a device attached to the access port to access the Voice VLAN.</td>
<td>From Cisco Unified Communications Manager Administration, choose Device &gt; Phone &gt; Phone Configuration.</td>
</tr>
<tr>
<td></td>
<td>Setting this option to No (disabled) prevents the attached PC from sending and receiving data on the Voice VLAN. This setting also prevents the PC from receiving data that the phone sends and receives.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Set this option to Yes (enabled) if an application that requires phone traffic monitoring is running on the PC. These applications include monitoring and recording applications and network monitoring software.</td>
<td></td>
</tr>
<tr>
<td>Web Access Enabled</td>
<td>Indicates whether web access is enabled (Yes) or disabled (No) for the phone.</td>
<td>For more information, see Control Web Page Access, on page 201.</td>
</tr>
<tr>
<td>Security Mode</td>
<td>Displays the security mode that is set for the phone.</td>
<td>Use Cisco Unified Communications Manager Administration to modify.</td>
</tr>
<tr>
<td>Logging Display</td>
<td>For use by the Cisco Technical Assistance Center (TAC), if necessary.</td>
<td></td>
</tr>
</tbody>
</table>

QoS Configuration Menu

The QoS Configuration menu displays information that relates to quality of service (QoS) for the phone. The following table describes the options on this menu.
Table 28: QoS Configuration Menu Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSCP For Call Control</td>
<td>Differentiated Services Code Point (DSCP) IP classification for call control signaling.</td>
<td>From Cisco Unified Communications Manager Administration, choose System &gt; Enterprise Parameters.</td>
</tr>
<tr>
<td>DSCP For Configuration</td>
<td>DSCP IP classification for any phone configuration transfer.</td>
<td>From Cisco Unified Communications Manager Administration, choose System &gt; Enterprise Parameters.</td>
</tr>
<tr>
<td>DSCP For Services</td>
<td>DSCP IP classification for phone-based services.</td>
<td>From Cisco Unified Communications Manager Administration, choose System &gt; Enterprise Parameters.</td>
</tr>
</tbody>
</table>

Related Topics

- Display Settings Menu, on page 62
- Network Configuration Menu, on page 66

Network Configuration Menu

The Network Configuration menu displays device-specific network configuration settings on the phone. The following table describes the options in this menu.

Note

The phone also has a Network Configuration menu that you access directly from the Settings menu. For information about the options on that menu, see Network Configuration Menu, on page 66.
### Table 29: Network Configuration Menu Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Load Server</td>
<td>Used to optimize installation time for phone firmware upgrades and offload the WAN by storing images locally, which negates the need to traverse the WAN link for each phone upgrade.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>You can set the Load Server to another TFTP server IP address or name (other than the TFTP Server 1 or TFTP Server 2) from which the phone firmware can be retrieved for phone upgrades. When the Load Server option is set, the phone contacts the designated server for the firmware upgrade.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The Load Server option allows you to specify an alternate TFTP server for phone upgrades only. The phone continues to use TFTP Server 1 or TFTP Server 2 to obtain configuration files. The Load Server option does not provide management of the process and of the files, such as file transfer, compression, or deletion.</td>
<td></td>
</tr>
<tr>
<td>RTP Control Protocol</td>
<td>Indicates whether the phone supports the Real-Time Control Protocol (RTCP). Settings include:</td>
<td>From Cisco Unified Communications Manager Administration, choose <strong>Device &gt; Phone &gt; Phone Configuration</strong>.</td>
</tr>
<tr>
<td></td>
<td>• Enabled</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Disabled (default)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If this feature is disabled, several call statistic values display as 0. For more information, see the following sections:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Call Statistics Screen</strong>, on page 193</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Streaming Statistics</strong>, on page 211</td>
<td></td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>To change</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| CDP: PC Port | Indicates whether CDP is enabled on the PC port (default is enabled).  
Enable CDP on the PC port when Cisco VT Advantage/Unified Video Advantage (CVTA) is connected to the PC port. CVTA does not work without CDP interaction with the phone.  
**Note** When CDP is disabled in Cisco Unified Communications Manager, a warning displays to indicate that disabling CDP on the PC port prevents CVTA from working. The current PC and switch port CDP values are shown on the Settings menu. | From Cisco Unified Communications Manager Administration, choose **Device > Phone**.                                                                                                                        |
| CDP: SW Port | Indicates whether CDP is enabled on the switch port (default is enabled).  
- Enable CDP on the switch port for VLAN assignment for the phone, power negotiation, QoS management, and 802.1x security.  
- Enable CDP on the switch port when the phone is connected to a Cisco switch.  
**Note** When CDP is disabled in Cisco Unified Communications Manager, a warning displays to indicate that CDP should be disabled on the switch port only if the phone connects to a non-Cisco switch. The current PC and switch port CDP values are shown on the Settings menu. | From Cisco Unified Communications Manager Administration, choose **Device > Phone**.                                                                                                                        |
The Peer Firmware Sharing feature provides these advantages in high speed campus LAN settings:

- Limits congestion on TFTP transfers to centralized remote TFTP servers.
- Eliminates the need to manually control firmware upgrades.
- Reduces phone downtime during upgrades when large numbers of devices are reset.

Peer Firmware Sharing may also aid in firmware upgrades in branch/remote office deployment scenarios over bandwidth-limited WAN links.

Enabling this setting allows the phone to discover similar phones on the subnet that are requesting the files that make up the firmware image, and to automatically assemble transfer hierarchies on a per-file basis. Only the root phone in the hierarchy retrieves the individual files that make up the firmware image from the TFTP server, and then the files are transferred down the transfer hierarchy to the other phones on the subnet by using TCP connections.

This menu option indicates whether the phone supports peer firmware sharing. Settings include:

- Enabled (default)
- Disabled

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer Firmware Sharing</td>
<td>The Peer Firmware Sharing feature provides these advantages in high speed campus LAN settings:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Limits congestion on TFTP transfers to centralized remote TFTP servers.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Eliminates the need to manually control firmware upgrades.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Reduces phone downtime during upgrades when large numbers of devices are reset.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Peer Firmware Sharing may also aid in firmware upgrades in branch/remote office deployment scenarios over bandwidth-limited WAN links.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enabling this setting allows the phone to discover similar phones on the subnet that are requesting the files that make up the firmware image, and to automatically assemble transfer hierarchies on a per-file basis. Only the root phone in the hierarchy retrieves the individual files that make up the firmware image from the TFTP server, and then the files are transferred down the transfer hierarchy to the other phones on the subnet by using TCP connections.</td>
<td></td>
</tr>
</tbody>
</table>

This menu option indicates whether the phone supports peer firmware sharing. Settings include:

- Enabled (default)
- Disabled

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Server</td>
<td>Indicates the IP address and port of the remote logging machine to which the phone sends log messages. These log messages help to debug the peer to peer image distribution feature.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Note The remote logging setting does not affect the sharing log messages that are sent to the phone log.</td>
<td></td>
</tr>
</tbody>
</table>

From Cisco Unified Communications Manager Administration, choose Device > Phone > Phone Configuration.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
</table>
| LLDP: PC Port        | Enables and disables Link Layer Discovery Protocol (LLDP) on the PC port. Use this setting to force the phone to use a specific discovery protocol. Settings include:  
\item Enabled (default)  
\item Disabled | From Cisco Unified Communications Manager Administration, choose Device > Phone > Phone Configuration. |
| LLDP-MED: SW Port    | Enables and disables Link Layer Discovery Protocol Media Endpoint Discovery (LLDP-MED) on the switch port. Use this setting to force the phone to use a specific discovery protocol, which should match the protocol supported by the switch. Settings include:  
\item Enabled (default)  
\item Disabled | From Cisco Unified Communications Manager Administration, choose Device > Phone > Phone Configuration. |
| LLDP Asset ID        | Identifies the asset ID assigned to the phone for inventory management.     | From Cisco Unified Communications Manager Administration, choose Device > Phone > Phone Configuration.                                      |
| Wireless Headset     | Enables users to receive notifications of incoming calls and answer or end calls while they work in a wireless environment. | From Cisco Unified Communications Manager Administration, choose Device > Phone > Phone Configuration.                                      |
| Hookswitch Control   | Advertises the phone power priority to the switch, which enables the switch to appropriately provide power to the phone. Settings include:  
\item Unknown (default)  
\item Low  
\item High  
\item Critical | From Cisco Unified Communications Manager Administration, choose Device > Phone > Phone Configuration. |
<p>| IP Addressing Mode   | Displays the IP addressing mode that is available on the phone. IPv4 only, IPv6 only, or IPv4 and IPv6. | From Cisco Unified Communications Manager Administration, choose Device &gt; Device Settings &gt; Common Device Configuration. |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
</table>
| IP Preference Mode Control   | Indicates the IP address version that the phone uses during signaling with Cisco Unified Communications Manager when both IPv4 and IPv6 are available on the phone. The IP addressing mode preference is configured on Cisco Unified Communications Manager Administration. Displays one of the following options on the phone:  
  - IPv4: The dual-stack phone prefers to establish a connection via an IPv4 address during a signaling event.  
  - IPv6: The dual-stack phone prefers to establish a connection via an IPv6 address during a signaling event. | From Cisco Unified Communications Manager Administration, choose Device > Device Settings > Common Device Configuration.                                                                                                                                          |
| Auto IP Configuration        | Displays whether the auto configurations is enabled or disabled on the phone. The Auto IP Configuration setting along with the DHCPv6 setting determine how the IP phone obtains the IPv6 address and other network settings. For more information on how these two settings affect the network settings on the phone, see DHCPv6 and Autoconfiguration, on page 84. | From Cisco Unified Communications Manager Administration, choose Device > Device Settings > Common Device Configuration.                                                                                                                                          |

**Note**

Use the "Allow Auto Configuration for Phones" setting in Cisco Unified Communications Manager Administration.
To change Description Option From Cisco Unified Communications Manager Administration, choose Device > Phone > Phone Configuration.

**Option** | **Description** | **To change**
--- | --- | ---
IPv6 Load Server | Used to optimize installation time for phone firmware upgrades and offload the WAN by storing images locally, which negates the need to traverse the WAN link for each phone upgrade. You can set the Load Server to another TFTP server IP address or name (other than the IPv6 TFTP Server 1 or IPv6 TFTP Server 2) from which the phone firmware can be retrieved for phone upgrades. When the Load Server option is set, the phone contacts the designated server for the firmware upgrade. **Note** The Load Server option allows you to specify an alternate TFTP server for phone upgrades only. The phone continues to use IPv6 TFTP Server 1 or IPv6 TFTP Server 2 to obtain configuration files. The Load Server option does not provide management of the process and of the files, such as file transfer, compression, or deletion. | From Cisco Unified Communications Manager Administration, choose Device > Phone > Phone Configuration.

IPv6 Log Server | Indicates the IP address and port of the remote logging machine to which the phone sends log messages. These log messages help to debug the peer to peer image distribution feature. **Note** The remote logging setting does not affect the sharing log messages that are sent to the phone log. | From Cisco Unified Communications Manager Administration, choose Device > Phone > Phone Configuration.

**Related Topics**

- Display Settings Menu, on page 62
- Network Configuration Menu, on page 66

**Security Configuration Menu**

The Security Configuration that you access directly from the Settings menu provides information about various security settings. It also provides access to the Trust List menu. This menu indicates if the CTL or ITL file is installed on the phone.
For information about how to access the Security Configuration menu and its submenus, see Display Settings Menu, on page 62.

The phone also has a Security Configuration menu that you access from the Device menu. For information about the security options on that menu, see Security Configuration Menu, on page 101.

The following table describes the options in the security configuration menu.

### Table 30: Security Configuration Menu Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Access Enabled</td>
<td>Indicates whether web access is enabled (Yes) or disabled (No) for the phone.</td>
<td>For more information, see Control Web Page Access, on page 201.</td>
</tr>
<tr>
<td>Security Mode</td>
<td>Displays the security mode that is set for the phone.</td>
<td>From Cisco Unified Communications Manager Administration, choose Device &gt; Phone &gt; Phone Configuration.</td>
</tr>
<tr>
<td>MIC</td>
<td>Indicates whether a manufacturing installed certificate (used for the security features) is installed on the phone (Yes) or is not installed on the phone (No).</td>
<td>For information about how to manage the MIC for your phone, see the “Using the Certificate Authority Proxy Function” chapter in the Cisco Unified Communications Manager Security Guide.</td>
</tr>
<tr>
<td>LSC</td>
<td>Indicates whether a locally significant certificate (used for the security features) is installed on the phone (Yes) or is not installed on the phone (No).</td>
<td>For information about how to manage the LSC for your phone, see the “Using the Certificate Authority Proxy Function” chapter in the Cisco Unified Communications Manager Security Guide.</td>
</tr>
</tbody>
</table>
**CTL File Submenu**

The CTL File screen includes the options that are described in the following table.

If a CTL file is installed on the phone, you can access the CTL File menu by pressing the **Settings** button and choosing **Security Configuration > Trust List**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust List</td>
<td>The Trust List is a top-level menu that provides submenus for the CTL, ITL, and Signed Configuration files. The CTL File submenu displays the contents of the CTL file. The ITL File submenu displays contents of the ITL file. The CTL and ITL files submenus also display the MD5 hash of the file. The MD5 hash value from the phone can be compared with the MD5 hash value of the file from the TFTP server to verify if the correct file is installed on the phone. The Signed Configuration File submenu displays the SRST certificate that is installed via the authenticated digitally signed configuration file.</td>
<td>For more information, see <strong>Trust List Menu, on page 115.</strong></td>
</tr>
<tr>
<td>802.1X Authentication</td>
<td>Allows you to enable 802.1X authentication for this phone.</td>
<td>See <strong>802.1X Authentication and Status Menus, on page 116.</strong></td>
</tr>
<tr>
<td>802.1X Authentication Status</td>
<td>Displays real-time status progress of the 802.1X authentication transaction.</td>
<td>Display only. Cannot configure.</td>
</tr>
<tr>
<td>VPN Configuration</td>
<td>Allows you to configure VPN configuration for this phone. (Supported only for the Cisco Unified IP Phone 7945G, 7965G, and 7975G.)</td>
<td>For more information, see the &quot;Configuring Virtual Private Networks&quot; chapter in <em>Cisco Unified Communications Manager Security Guide</em>.</td>
</tr>
</tbody>
</table>
### Table 31: CTL File Menu Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTL File</td>
<td>Displays the MD5 hash of the CTL file that is installed in the phone. If</td>
<td>For more information about the CTL file, see the &quot;Configuring the Cisco CTL Client&quot; chapter in the <em>Cisco Unified Communications Manager Security Guide</em>.</td>
</tr>
<tr>
<td></td>
<td>security is configured for the phone, the CTL file installs automatically</td>
<td></td>
</tr>
<tr>
<td></td>
<td>when the phone reboots or resets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• A locked padlock icon <img src="https://example.com/padlock.png" alt="padlock" /> in this</td>
<td></td>
</tr>
<tr>
<td></td>
<td>option indicates that the CTL file is locked.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• An unlocked padlock icon <img src="https://example.com/padlock.png" alt="padlock" /></td>
<td></td>
</tr>
<tr>
<td></td>
<td>indicates that the CTL file is unlocked.</td>
<td></td>
</tr>
<tr>
<td>CAPF Server</td>
<td>Common Name (from the Cisco Unified Communications Manager Certificate) of</td>
<td>For more information about this server, see the “Using the Certificate Authority Proxy Function” chapter in the <em>Cisco Unified Communications Manager Security Guide</em>.</td>
</tr>
<tr>
<td></td>
<td>the CAPF used by the phone. Also displays a certificate <img src="https://example.com/certificate.png" alt="certificate" /> icon if a certificate is installed for this server.</td>
<td></td>
</tr>
<tr>
<td>Unified CM/TFTP</td>
<td>Common Name (from the Cisco Unified Communications Manager Certificate) of a</td>
<td>For information about these options, see Network Configuration Menu, on page 66.</td>
</tr>
<tr>
<td>Server</td>
<td>Cisco Unified Communications Manager and TFTP server used by the phone.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Also displays a certificate <img src="https://example.com/certificate.png" alt="certificate" /> icon if a certificate is installed for this server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If the certificate of the TFTP (TFTP Server 1) or the backup TFTP (TFTP Server 2) is not in the CTL or ITL file, one of the files must be unlocked.</td>
<td></td>
</tr>
</tbody>
</table>
To change
Description
Option
Common Name (from the Cisco
Unified Communications Manager
Certificate) of the trusted application
server used by the phone. Also
displays a certificate 🕵️ icon.
A phone-trust certificate is used to
authenticate application servers with
which the phone communicates.
One Application Server menu item
appears for each phone-trust store
whose certificates have been
uploaded into Cisco Unified OS
Administration and later downloaded
into the phone CTL file.

To more information about phone-trust
certificates, see the following documents:

• Cisco Unified Communications
  Operating System Administration

• Cisco Unified Communications Manager
  chapter

Unlock CTL and ITL Files

To unlock the CTL and ITL files from the Security Configuration menu, perform these steps:

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Press **# to unlock options on the overall setting menu of the Cisco Unified IP Phone.</th>
</tr>
</thead>
</table>
| Step 2 | Select Trust List > CTL or ITL file depending on which file is installed in your phone.  
**Note** If both CTL and ITL files are installed in your phone, you can choose either option. |
| Step 3 | Press Unlock to unlock Trust List files on the phone. The CTL or ITL files, if installed on your phone, will be unlocked together.  
**Note** When you press Unlock, the softkey changes to Lock. If you decide not to change the TFTP server option, press Lock to lock the CTL file. |

ITL File Submenu

The ITL File screen includes the options that are described in the following table.

If an ITL file is installed on the phone, you can access the ITL File submenu by pressing the Settings button and choosing Security Configuration > Trust List.

**Note** The TFTP server generates the ITL file. The Trust Verification Service does not generate the ITL file, as done in previous releases.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITL File</td>
<td>Displays the MD5 hash of the Identity Trust List (ITL) file that is installed in the phone. If security is configured for the phone, the ITL file installs automatically when the phone reboots or resets.</td>
<td>For more information about the ITL file, see the &quot;Configuring the Cisco ITL Client&quot; chapter in the <em>Cisco Unified Communications Manager Security Guide</em>.</td>
</tr>
<tr>
<td></td>
<td>* A locked padlock icon in this option indicates that the ITL file is locked.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>* An unlocked padlock icon indicates that the ITL file is unlocked.</td>
<td></td>
</tr>
<tr>
<td>CAPF Server</td>
<td>Common Name (from the Cisco Unified Communications Manager Certificate) of the CAPF used by the phone. Also displays a certificate icon if a certificate is installed for this server.</td>
<td>For more information about this server, see the &quot;Using the Certificate Authority Proxy Function&quot; chapter in the <em>Cisco Unified Communications Manager Security Guide</em>.</td>
</tr>
<tr>
<td>Unified CM/TFTP Server</td>
<td>Common Name (from the Cisco Unified Communications Manager Certificate) of a Cisco Unified Communications Manager and TFTP server used by the phone. Also displays a certificate icon if a certificate is installed for this server. If neither the certificate of TFTP (TFTP Server 1) nor the certificate of backup TFTP (TFTP Server 2) is in the CTL or ITL file, you must unlock the CTL file or the ITL file.</td>
<td>For information about changing these options, see <em>Network Configuration Menu</em>, on page 66.</td>
</tr>
</tbody>
</table>
| Application Server  | Common Name (from the Cisco Unified Communications Manager Certificate) of the trusted application server used by the phone. Also displays a certificate icon. A phone-trust certificate is used to authenticate application servers with which the phone communicates. One Application Server menu item appears for each phone-trust store whose certificates have been uploaded into Cisco Unified OS Administration and later downloaded into the Phone ITL file. | For more information about phone-trust certificates, see the following documents:  
  * *Cisco Unified Communications Operating System Administration Guide*, "Security" chapter  
  * *Cisco Unified Communications Manager Security Guide*, "Security Overview" chapter |

For more information about phone-trust certificates, see the following documents:

- *Cisco Unified Communications Operating System Administration Guide*, "Security" chapter
- *Cisco Unified Communications Manager Security Guide*, "Security Overview" chapter
**Option** | **Description** | **To change**
--- | --- | ---
Trust Verification Service Server | Common Name (from the Cisco Unified Communications Manager Certificate) of the trusted application server used by the phone. Also displays a certificate icon. A phone-trust TVS certificate is used to authenticate TVS servers with which the phone communicates. There can be more than one entry for the TVS servers. | For more information, see the *Cisco Unified Communications Manager System Administrator Guide*. |

**Trust List Menu**

The Trust List menu provides a top-level menu that contains the CTL, ITL, and the Signed Configuration submenus. The content of the Signed Configuration file is SRST.

The Trust List menu displays information about all of the servers that the phone trusts and includes the options that are described in the following table.

**Table 33: Trust List Menu Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAPF Server</td>
<td>Common Name (from the Cisco Unified Communications Manager Certificate) of the CAPF server used by the phone. Also displays a certificate icon if a certificate is installed for this server.</td>
<td>For more information about these settings, see the &quot;Configuring the Cisco ITL Client&quot; chapter in the <em>Cisco Unified Communications Manager Security Guide</em>.</td>
</tr>
<tr>
<td>Unified CM/TFTP Server</td>
<td>Common Name (from the Cisco Unified Communications Manager Certificate) of a Cisco Unified Communications Manager and the TFTP server used by the phone. Also displays a certificate icon if a certificate is installed for this server.</td>
<td>For more information about these settings, see the &quot;Configuring the Cisco ITL Client&quot; chapter in the <em>Cisco Unified Communications Manager Security Guide</em>.</td>
</tr>
<tr>
<td>SRST Router</td>
<td>Common Name (from the Cisco Unified Communications Manager Certificate) of the trusted SRST router that is available to the phone, if such a device has been configured in Cisco Unified Communications Manager Administration. Also displays a certificate icon if a certificate is installed for this server.</td>
<td>For more information about these settings, see the &quot;Configuring the Cisco ITL Client&quot; chapter in the <em>Cisco Unified Communications Manager Security Guide</em>.</td>
</tr>
</tbody>
</table>
### Option | Description | To change
--- | --- | ---
Application Server | Common Name (from the Cisco Unified Communications Manager Certificate) of the trusted application server used by the phone. Also displays a certificate icon. A phone-trust certificate is used to authenticate application servers with which the phone communicates. One Application Server menu item appears for each phone-trust store whose certificates have been uploaded into Cisco Unified OS Administration and later downloaded into the Cisco Unified IP Phone CTL file. | For more information about phone-trust certificates, see the following documents:
- **Cisco Unified Communications Operating System Administration Guide**, “Security” chapter
- **Cisco Unified Communications Manager Security Guide**, “Security Overview” chapter

TVS Server | Common Name (from the Cisco Unified Communications Manager Certificate) of the trusted application server used by the phone. Also displays a certificate icon. A phone-trust TVS certificate is used to authenticate TVS servers with which the phone communicates. There can be more than one entry for the TVS servers. | For more information, see the **Cisco Unified Communications Manager System Administrator Guide**.

### 802.1X Authentication and Status Menus

The 802.1X Authentication and 802.1X Authentication Status menus allow you to enable 802.1X authentication and monitor the progress. These options are described in the following tables.

You can access the 802.1X Authentication settings by pressing the Settings button and choosing Security Configuration > 802.1X Authentication. To exit this menu, press Exit.

#### Table 34: 802.1X Authentication Menu Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
</table>
| Device Authentication | Determines whether 802.1X authentication is enabled:  
- Enabled: Phone uses 802.1X authentication to request network access.  
- Disabled: Default setting in which the phone uses CDP to acquire VLAN and network access. | Voice Quality Troubleshooting Tips, on page 240 |
To access the 802.1X Authentication Real-Time menu, press the Settings button and choose Security Configuration > 802.1X Authentication Status. To exit this menu, press Exit.
### Table 35: 802.1X Authentication Status Menu Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1X Authentication</td>
<td>Real-time progress of the 802.1X authentication status. Displays one of the</td>
<td>Display only. Cannot configure.</td>
</tr>
<tr>
<td>Status</td>
<td>following states:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Disabled: 802.1X is disabled and the transaction was not attempted.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Disconnected: Physical link is down or is disconnected.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Connecting: System is trying to discover or acquire the authenticator.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Acquired: Authenticator has been acquired. System is waiting for</td>
<td></td>
</tr>
<tr>
<td></td>
<td>authentication to begin.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Authenticating: Authentication is in progress.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Authenticated: Authentication was successful or implicit authentication</td>
<td></td>
</tr>
<tr>
<td></td>
<td>occurred due to timeouts.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Held: Authentication failed. System is waiting before next attempt</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(approximately 60 seconds).</td>
<td></td>
</tr>
</tbody>
</table>

### Set Device Authentication Field

**Procedure**

1. **Step 1** Choose **Settings > Security Configuration > 802.1X Authentication > Device Authentication**.
2. **Step 2** Set the Device Authentication option to **Enabled** or **Disabled**.
3. **Step 3** Press **Save**.

### Set EAP-MD5 Shared Secret Field

See **Cisco Unified IP Phone Security Problems, on page 224** for recovery of a deleted shared secret.
Procedure

Step 1  Choose EAP-MD5 > Shared Secret.
Step 2  Enter the shared secret.
Step 3  Press Save.

VPN Configuration Menu

The VPN Configuration menu allows you to enable a virtual private network (VPN) connection that uses Secure Sockets Layer (SSL) when a phone is located outside a trusted network or when network traffic between the phone and Cisco Unified Communications Manager crosses untrusted networks.

Note

VPN Client is supported only for the Cisco Unified IP Phone 7945G, 7965G, and 7975G.

Your system administrator configures the VPN Client feature as needed. If it is enabled and the VPN Client mode is enabled on the phone, you are prompted for your credentials as follows:

- If your phone is located outside the corporate network:
  - You are prompted at login to enter your credentials based on the authentication method that your system administrator configured on your phone.

- If your phone is located inside the corporate network:
  - If Auto Network Detection is disabled, you are prompted for credentials, and a VPN connection is possible.
  - If Auto Network Detection is enabled, you cannot connect through VPN so you are not prompted.

Connect to VPN

Use this procedure to access the VPN Configuration settings and connect through VPN.

Procedure

Step 1  Press Settings and choose Security Configuration > VPN Configuration.
Step 2  After the phone starts up and the VPN Login screen appears, enter your credentials based on the configured authentication method:
  a) Username and password: Enter your username and the password that your system administrator gave you.
  b) Password and certificate: Enter the password that your system administrator gave you. Your username is derived from the certificate.
  c) Certificate: If the phone uses only a certificate for authentication, you do not need to enter authentication data. The VPN Login screen displays the status of the phone that is attempts the VPN connection.
When the power is lost or in some scenarios when the phone is reset, all stored credentials are removed.

**Step 3**  
To establish the VPN connection, press **Submit**.

**Step 4**  
To disable the VPN login process, press **Cancel**.

## VPN Configuration Fields

The following table shows the VPN Configuration menu options on the Cisco Unified IP Phone.

### Table 36: VPN Configuration Menu Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
</table>
| VPN               | Determines whether the VPN Client is enabled or disabled:                   | 1  Choose **Settings** > **Security Configuration** > **VPN Configuration** > **VPN**.  
<p>|                   | • Enable: Enables VPN feature. (When enabled, the Disable softkey is shown.)  | 2  Set the VPN option to Enabled or Disabled.                                |
|                   | • Disable: Disables VPN feature. (When disabled, the Enable softkey is shown.) | If the feature is disabled on Cisco Unified Communications Manager, this option is disabled. |
|                   | Settings do not have to be unlocked to set this option.                      |                                                                           |
| Clear Username and Password | Clears the current username and password.                                    | The option is inactive when the authentication method is certificate only, or if the feature is disabled on Cisco Unified Communications Manager. |
| Auto Network Detection | Shows whether option is Enabled or Disabled.                                | Display only. Configured on Cisco Unified Communications Manager.           |
| Concentrator 1    | Allows you to see if concentrator 1, 2, or 3 is Connected or Inactive and view the concentrator details. | For configured concentrators, press <strong>Select</strong> to view concentrator details. |
| Concentrator 2    | In the VPN Configuration menu, choose <strong>Concentrator 1</strong>, <strong>Concentrator 2</strong>, or <strong>Concentrator 3</strong>, as desired: | A new screen appears that has a title of &quot;Concentrator X,&quot; where X is the concentrator number. The URL configured for the concentrator is displayed in the window with the link to the URL on the first line and the URL itself on the second line. |
| Concentrator 3    |                                                                           |                                                                           |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Mode</td>
<td>Shows the authentication method:</td>
<td>Display only. Configured on Cisco Unified Communications Manager.</td>
</tr>
<tr>
<td></td>
<td>• Certificate</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Username and Password</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Password and Certificate</td>
<td></td>
</tr>
<tr>
<td>Encryption Method</td>
<td>Shows the encryption method if the VPN tunnel is connected:</td>
<td>Displays the encryption method only if a VPN tunnel is connected; otherwise, no value displays.</td>
</tr>
<tr>
<td></td>
<td>• AES128-SHA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• AES256-SHA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• DES-CBC3-SHA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If VPN is not connected, no method is shown.</td>
<td></td>
</tr>
</tbody>
</table>
Features, Templates, Services, and Users Overview

After you install Cisco Unified IP Phones in your network, configure their network settings, and add them to Cisco Unified Communications Manager, you must use Cisco Unified Communications Manager Administration to configure telephony features, optionally modify phone templates, set up services, and assign users.

This chapter provides an overview of these configuration and setup procedures. Cisco Unified Communications Manager documentation provides detailed instructions for these procedures.

For suggestions about how to provide users with information about features, and what information to provide, see Internal Support Web Site, on page 243.

For information about setting up phones in non-English environments, see International User Support, on page 259.
Telephony Features Available for Cisco Unified IP Phone

After you add Cisco Unified IP Phones to Cisco Unified Communications Manager, you can add functionality to the phones. The following table includes a list of supported telephony features, many of which you configure by using Cisco Unified Communications Manager Administration. The Configuration reference column lists Cisco Unified Communications Manager documentation that contain configuration procedures and related information.

For information about using most of these features on the phone, see Cisco Unified IP Phone 7975G, 7971G-GE, 7970G, 7965G, and 7945G User Guide for Cisco Unified Communications Manager (SCCP and SIP).

Note

Cisco Unified Communications Manager Administration also provides several service parameters that you can use to configure various telephony functions. For more information about service parameters and the functions that they control, see the Cisco Unified Communications Manager Administration Guide.

Table 37: Telephony Features for the Cisco Unified IP Phone

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Configuration reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abbreviated Dialing</td>
<td>Allows users to speed dial a phone number by entering an assigned index code (1-99) on the phone keypad.</td>
<td>For more information, see:</td>
</tr>
<tr>
<td></td>
<td>You can use Abbreviated Dialing while on-hook or off-hook.</td>
<td>• Cisco Unified Communications Manager Administration Guide, &quot;Cisco Unified IP Phone Configuration&quot; chapter</td>
</tr>
<tr>
<td></td>
<td>Users assign index codes from the User Options web pages.</td>
<td>• Cisco Unified Communications Manager System Guide, &quot;Cisco Unified IP Phones&quot; chapter.</td>
</tr>
</tbody>
</table>

Note
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Configuration reference</th>
</tr>
</thead>
</table>
| Agent Greeting          | Allows an agent or administrator to create and play a prerecorded greeting automatically at the beginning of a call, such as a customer call, before the agent begins the conversation with the caller. An Agent can prerecord a single greeting or multiple ones as needed and create and update them. When a customer calls, both callers hear the prerecorded greeting. The agent can remain on mute until the greeting ends or answer the call over the greeting. All codecs supported for the phone are supported for Agent Greeting calls. To enable Agent Greeting in the Cisco Unified Communications Manager Administration application, choose Device > Phone, locate IP Phone that you want to configure. Scroll to the Device Information Layout pane and set Builtin Bridge to On or Default. If Builtin Bridge is set to Default, in the Cisco Unified Communications Manager Administration application, choose System > Service Parameter and select the appropriate Server and Service. Scroll to the Clusterwide Parameters (Device - Phone) pane and set Builtin Bridge Enable to On. | For more information, see:  
  - *Cisco Unified Communications Manager Features and Services Guide*, "Barge and Privacy" chapter  
  - *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones" chapter |
<p>| Anonymous Call Block    | Allows a user to reject calls from anonymous callers.                       | For more information, see the <em>Cisco Unified Communications Manager Administration Guide</em>, &quot;SIP Profile Configuration&quot; chapter. |
| (SIP phones only)       |                                                                             |                                                                                                                                                    |
| Any Call Pickup         | Allows users to pick up a redirected call via a CTI application, on any line in their call pickup group, regardless of how the call was routed to the phone. | For more information, see the <em>Cisco Unified Communications Manager Features and Services Guide</em>, &quot;Call Pickup&quot; chapter. |
| Assisted Directed Call  | 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. | For more information, see the <em>Cisco Unified Communications Manager Features and Services Guide</em>, &quot;Assisted Directed Call Park&quot; chapter. |</p>
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Configuration reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audible Message Waiting Indicator</td>
<td>A stutter tone from the handset, headset, or speakerphone indicates that a user has one or more new voice messages on a line.</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>The stutter tone is line-specific. You hear it only when using the line with the waiting messages.</td>
<td>For more information, see:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <em>Cisco Unified Communications Manager Administration Guide</em>, “Message Waiting Configuration” chapter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <em>Cisco Unified Communications Manager System Guide</em>, “Voice Mail Connectivity to Cisco Unified Communications Manager” chapter</td>
</tr>
<tr>
<td>AutoAnswer</td>
<td>Connects incoming calls automatically after a ring or two. AutoAnswer works with either the speakerphone or the headset.</td>
<td>For more information, see the <em>Cisco Unified Communications Manager Administration Guide</em>, “Directory Number Configuration” chapter.</td>
</tr>
<tr>
<td>Auto Dial</td>
<td>Allows the phone user to choose from matching numbers in the Placed Calls log while dialing. To place the call, the user can choose a number from the Auto Dial list or continue to enter digits manually.</td>
<td>No configuration required.</td>
</tr>
<tr>
<td>Auto Call Pickup</td>
<td>Allows a user to use one-touch pickup functionality for call pickup features.</td>
<td>For more information, see the <em>Cisco Unified Communications Manager Features and Services Guide</em>, “Call Pickup” chapter.</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Configuration reference</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Automatic Port Synchronization | When the Cisco Unified Communications Manager administrator uses the Remote Port Configuration feature to set the speed and duplex function of an IP phone remotely, loss of packets can occur if one port is slower than the other. 

The Automatic Port Synchronization feature synchronizes the ports to the lowest speed among the two ports, which eliminates packet loss. When automatic port synchronization is enabled, it is recommended that both ports be configured for autonegotiate. If one port is enabled for autonegotiate and the other is at a fixed speed, the phone synchronizes to the fixed port speed. 

**Note** If both the ports are configured for fixed speed, the Automatic Port Synchronization feature is ineffective. 

**Note** The Remote Port Configuration and Automatic Port Synchronization features are compatible only with IEEE 802.3AF Power of Ethernet (PoE) switches. Switches that support only Cisco Inline Power are not compatible. Enabling this feature on phones that are connected to these types of switches could result in loss of connectivity to Cisco Unified Communications Manager, if the phone is powered by PoE. | To configure the parameter in the Cisco Unified Communications Manager Administration application, choose Device > Phone, select the appropriate IP phones, and scroll to the Product Specific Configuration Layout pane. 

To configure the setting on multiple phones simultaneously, enable Automatic Port Synchronization in the Enterprise Phone Configuration (System > Enterprise Phone Configuration). |
| Barge (and cBarge) | Allows a user to join a nonprivate call on a shared phone line. Barge features include cBarge and Barge. 

- cBarge adds a user to a call and converts it into a conference, allowing the user and other parties to access conference features. 
- Barge adds a user to a call but does not convert the call into a conference. 

The phones support Barge in two conference modes: 

- Built-in conference bridge at the target device (the phone that is being barged). This mode uses the **Barge** softkey. 
- Shared conference bridge. This mode uses the **cBarge** softkey. | For more information, see: 

- Cisco Unified Communications Manager Administration Guide, “Cisco Unified IP Phone Configuration” chapter 
- Cisco Unified Communications Manager System Guide, “Cisco Unified IP Phones” chapter 
- Cisco Unified Communications Manager Features and Services Guide, “Barge and Privacy” chapter |
<p>| Block External to External Transfer | Prevents users from transferring an external call to another external number. | For more information, see the Cisco Unified Communications Manager Features and Services Guide, “External Call Transfer Restrictions” chapter. |</p>
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Configuration reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Busy Lamp Field (BLF)</td>
<td>Allows a user to monitor the call state of a directory number associated with a speed-dial button, call log, or directory listing on the phone.</td>
<td>For more information, see the Cisco Unified Communications Manager Features and Services Guide, “Presence” chapter.</td>
</tr>
<tr>
<td>Busy Lamp Field (BLF) Pickup</td>
<td>Provides enhancements to BLF speed dial. Allows you to configure a directory number (DN) that a user can monitor for incoming calls. When the DN receives an incoming call, the system alerts the monitoring user, who can then pick up the call.</td>
<td>For more information, see the Cisco Unified Communications Manager Feature and Services Guide, “Call Pickup” chapter.</td>
</tr>
</tbody>
</table>
| Call Back | Provides users with an audio and visual alert on the phone when a busy or unavailable party becomes available. | For more information, see:  
- Cisco Unified Communications Manager System Guide, “Cisco Unified IP Phones” chapter  
- Cisco Unified Communications Manager Features and Services Guide, “CallBack” chapter |
| Call Chaperone | Allows an authorized Chaperone user to supervise and record a call.  
The Call Chaperone user intercepts and answers the call from the calling party, manually creates a conference to the called party, and remains on the conference to supervise and record the call. Cisco Unified IP Phones that have the Call Chaperone feature configured on them have a Record softkey. The Call Chaperone user presses the Record softkey to record a call.  
For chaperoned calls, an announcement is played or spoken by one of the participants at the start of the call. An announcement alerts later participants that the call is being recorded.  
The Call Chaperone feature is supported only with External Call Control, which allows Cisco Unified Communications Manager to route audio and video calls to a route server that hosts routing rules. | For more information, see the Cisco Unified Communications Manager Features and Services Guide, “External Call Control” chapter. |
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Configuration reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Display Restrictions</td>
<td>Determines the information that will display for calling or connected lines, depending on the parties who are involved in the call.</td>
<td>For more information, see:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <em>Cisco Unified Communications Manager Administration Guide</em>, &quot;Cisco Unified IP Phone Configuration&quot; chapter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <em>Cisco Unified Communications Manager System Guide</em>, “Understanding Route Plans” chapter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <em>Cisco Unified Communications Manager Features and Services Guide</em>, &quot;Call Display Restrictions&quot; chapter</td>
</tr>
<tr>
<td>Call Forward</td>
<td>Allows users to redirect incoming calls to another number. Call Forward options include Call Forward All, Call Forward Busy, Call Forward No Answer, and Call Forward No Coverage.</td>
<td>For more information, see:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <em>Cisco Unified Communications Manager Administration Guide</em>, &quot;Directory Number Configuration&quot; chapter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <em>Cisco Unified Communications Manager System Guide</em>, &quot;Cisco Unified IP Phones&quot; chapter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <em>User Options Web Pages Options</em>, on page 158</td>
</tr>
<tr>
<td>Call Forward All Destination Override</td>
<td>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.</td>
<td>For more information, see the <em>Cisco Unified Communications Manager System Guide</em>, &quot;Understanding Directory Numbers&quot; chapter</td>
</tr>
<tr>
<td>Call Forward All Loop Breakout</td>
<td>Detects and prevents Call Forward All loops. When a Call Forward All loop is detected, the Call Forward All configuration is ignored and the call rings through.</td>
<td>For more information, see the <em>Cisco Unified Communications Manager System Guide</em>, &quot;Cisco Unified IP Phones&quot; chapter</td>
</tr>
<tr>
<td>Call Forward All Loop Prevention</td>
<td>Prevents a user from configuring a Call Forward All destination directly on the phone that creates a Call Forward All loop or that creates a Call Forward All chain with more hops than the existing Forward Maximum Hop Count service parameter allows.</td>
<td>For more information, see the <em>Cisco Unified Communications Manager System Guide</em>, &quot;Cisco Unified IP Phones&quot; chapter</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Configuration reference</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Call Forward Configurable Display | Allows you to specify information that appears on a phone when a call is forwarded. This information can include the caller name, caller number, redirected number, and original dialed number. | For more information, see:  
• *Cisco Unified Communications Manager Administration Guide*  
• *Cisco Unified Communications Manager System Guide*, “Cisco Unified IP Phones” chapter |
| Calling Party Normalization | Globalizes or localizes the incoming calling party number so that the appropriate calling number presentation displays on the phone. Supports the international escape character +. | For more information, see the *Cisco Unified Communications Features and Services Guide*, “Calling Party Normalization” chapter. |
| Call Park               | Allows users to park (temporarily store) a call and then retrieve the call by using another phone in the Cisco Unified Communications Manager system.                                                          | For more information, see the *Cisco Unified Communications Manager Features and Services Guide*, “Call Park and Directed Call Park” chapter. |
| 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/or visual alert for the primary line on the phone. This alert notifies the users that a call is ringing in their pickup group. | For more information, see the *Cisco Unified Communications Manager Features and Services Guide*, “Call Pickup” chapter. |
| Call Recording          | Allows a supervisor to record an active call. The user might hear a recording audible alert tone during a call when it is being recorded.  
When a call is secured, the security status of the call is displayed as a lock icon on Cisco Unified IP Phones. The connected parties might also hear an audible alert tone that indicates the call is secured and is being recorded.  
**Note** When an active call is being monitored or recorded, you can receive or place intercom calls; however, if you 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. | For more information, see the *Cisco Unified Communications Manager Features and Services Guide*, “Monitoring and Recording” chapter. |
<p>| Call Waiting            | Indicates and allows users to answer an incoming call that rings while on another call. Displays incoming call information on the phone screen.                                                                          | For more information, see the <em>Cisco Unified Communications System Guide</em>, “Understanding Directory Numbers” chapter. |</p>
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Configuration reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Caller ID</td>
<td>Displays caller identification such as a phone number, name, or other</td>
<td>For more information, see:</td>
</tr>
<tr>
<td></td>
<td>descriptive text on the phone screen.</td>
<td>• <em>Cisco Unified Communications Manager Administration Guide</em>, &quot;Cisco Unified IP Phone</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configuration&quot; chapter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <em>Cisco Unified Communications Manager System Guide</em>, &quot;Understanding Route Plans&quot; chapter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <em>Cisco Unified Communications Manager Features and Services Guide</em>,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;Call Display Restrictions&quot; chapter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <em>Cisco Unified Communications Manager Administration Guide</em>, &quot;Directory Number</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configuration&quot; chapter</td>
</tr>
<tr>
<td>Cisco Extension Mobility</td>
<td>Allows a user temporarily to apply a phone number and user profile</td>
<td>For more information, see the *Cisco Unified Communications Manager Features</td>
</tr>
<tr>
<td></td>
<td>settings to a shared Cisco Unified IP Phone by logging into the Extension</td>
<td>and Services Guide*, &quot;Cisco Extension Mobility&quot; chapter.</td>
</tr>
<tr>
<td></td>
<td>Mobility service on that phone.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Extension Mobility can be useful if users work from a variety of</td>
<td></td>
</tr>
<tr>
<td></td>
<td>locations within your company or if they share a workspace with</td>
<td></td>
</tr>
<tr>
<td></td>
<td>coworkers.</td>
<td></td>
</tr>
<tr>
<td>Cisco Extension Mobility</td>
<td>Enables a user to change the PIN from a Cisco Unified IP Phone. The PIN</td>
<td>For more information, see the *Cisco Unified Communications Manager Features and</td>
</tr>
<tr>
<td>Change PIN</td>
<td>can be changed by:</td>
<td>Services Guide*, &quot;Cisco Extension Mobility&quot; chapter.</td>
</tr>
<tr>
<td></td>
<td>• Using the Change Credentials service of a Cisco Unified IP Phone</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Using the <strong>ChangePIN</strong> softkey on the Extension Mobility logout screen</td>
<td></td>
</tr>
<tr>
<td>Cisco Extension Mobility</td>
<td>Enables a user configured in one cluster to log into a Cisco Unified IP</td>
<td>For more information, see the *Cisco Unified Communications Manager Features and</td>
</tr>
<tr>
<td>Cross Cluster</td>
<td>Phone in another visiting cluster.</td>
<td>Services Guide*, &quot;Cisco Extension Mobility Cross Cluster&quot; chapter.</td>
</tr>
<tr>
<td></td>
<td>Users from a home cluster log into a Cisco Unified IP Phone at a visiting</td>
<td></td>
</tr>
<tr>
<td></td>
<td>cluster.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Even though the Intercom feature works with Cisco Extension</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mobility (EM), it cannot be used with EMCC because the feature must be</td>
<td></td>
</tr>
<tr>
<td></td>
<td>enabled with a real phone device. The Intercom feature cannot be enabled</td>
<td></td>
</tr>
<tr>
<td></td>
<td>with EM profiles.</td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Configuration reference</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Cisco Unified Communications Manager Assistant</td>
<td>Enables managers and their assistants to work together more effectively by providing a call-routing service, enhancements to phone capabilities for the manager, and desktop interfaces that are primarily used by the assistant.</td>
<td>For more information, see the <em>Cisco Unified Communications Manager Features and Services Guide</em>, “Cisco Unified Communications Manager Assistant with Proxy Line Support” and “Cisco Unified Communications Manager Assistant with Shared Line Support” chapters.</td>
</tr>
<tr>
<td>Client Matter Codes (CMC) (SCCP phones only)</td>
<td>Enables a user to specify that a call relates to a specific client matter.</td>
<td>For more information, see the <em>Cisco Unified Communications Manager Features and Services Guide</em>, “Client Matter Codes and Forced Authorization Codes” chapter.</td>
</tr>
<tr>
<td>Computer Telephony Integration (CTI) Applications</td>
<td>A computer telephony integration (CTI) route point can designate a virtual device to receive multiple, simultaneous calls for application-controlled redirection.</td>
<td>For more information, see the <em>Cisco Unified Communications Manager Administration Guide</em>, “CTI Route Point Configuration” chapter.</td>
</tr>
</tbody>
</table>
| Conference                                   | Allows a user to talk simultaneously with multiple parties by calling each participant individually. Conference features include Conference, Join, eBarge, and Meet-Me. 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. | For more information, see: *Cisco Unified Communications Manager System Guide*, “Cisco Unified IP Phones” chapter  
* The service parameter, Advanced Adhoc Conference (disabled by default in Cisco Unified Communications Manager Administration), allows you to enable these features.  
   **Note** Be sure to inform your users whether these features are activated.                                                                                                             |
| Control Default Wallpaper                    | Administrators can specify the default background image file for the phone in the Cisco Unified Communication Manager administration console administration console. The image is set as the background image only if the administrator has disabled the Enable End User Access to Phone Background Image Setting checkbox. | For more information, see the *Cisco Unified Communications Manager Features and Services Guide*, “Common Phone Profile Configuration” chapter.                                                                            |
| Default Audio Path Support                   | Allows the user to press Answer or a Line button for, and redirect the call to, the last audio path used, by default.                                                                                           | No configuration required.                                                                                                                                                                                                 |
| Device Invoked Recording                     | Provides end users with the ability to record their telephone calls via a softkey. In addition administrators may continue to record telephone calls via the CTI User Interface.                                      | For more information, see Enable Device Invoked Recording, on page 156.                                                                                                                                                      |
### Telephony Features Available for Cisco Unified IP Phone

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Configuration reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directed Call Park</td>
<td>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. <strong>Note</strong> If you implement Directed Call Park, avoid configuring the Park softkey. This prevents users from confusing the two Call Park features.</td>
<td>For more information, see the <em>Cisco Unified Communications Manager Features and Services Guide</em>, “Call Park and Directed Call Park” chapter.</td>
</tr>
<tr>
<td>Direct Transfer</td>
<td>Allows users to connect two calls to each other (without remaining on the line).</td>
<td>For more information, see the <em>Cisco Unified Communications Manager System Guide</em>, “Cisco Unified IP Phones” chapter.</td>
</tr>
<tr>
<td>Directed Call Pickup</td>
<td>Allows a user to answer a call that is ringing on a particular directory number.</td>
<td>For more information, see the <em>Cisco Unified Communications Manager Features and Services Guide</em>, “Call Pickup” chapter.</td>
</tr>
<tr>
<td>Distinctive Ring</td>
<td>Users can customize how their phone indicates an incoming call and a new voice mail message. Users can customize up to six distinctive rings.</td>
<td>For more information, see the <em>Cisco Unified Communications Manager Features and Services Guide</em>, “Custom Phone Rings” chapter.</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Configuration reference</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 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. You can configure the phone to have a softkey template with a DND softkey or a phone-button template with DND as one of the selected features. The following DND-related parameters are configurable in Cisco Unified Communications Manager Administration:  
  - Do Not Disturb: Choose Device > Phone > Phone Configuration.  
  - DND Option: Choose "Call Reject" (to turn off all audible and visual notifications), or "Ringer Off" (to turn off only the ringer). DND Option appears on both the Common Phone Profile window and the Phone Configuration window (Phone Configuration window value takes precedence).  
  - DND Incoming Call Alert: Choose the type of alert to play, if any, on a phone for incoming calls when DND is active. This parameter is located on both the Common Phone Profile window and the Phone Configuration window (Phone Configuration window value takes precedence).  
  - BLF Status Depicts DND: Enables DND status to override busy/idle state. | For more information, see the *Cisco Unified Communications Manager Features and Services Guide*, “Do Not Disturb” chapter.                                |
<p>| Enbloc Dialing (SCCP phones only) | Enbloc dialing enables SCCP to send all digits of a phone number simultaneously. This feature must be disabled if either Forced Authorization Codes (FAC) or Client Matter Codes (CMC) dialing is being used.                                                                                                               | To disable enbloc dialing, in Cisco Unified Communications Manager Administration, go to Device &gt; Phone. On the Phone Configuration window, in the Product Specific Configuration Layout area, uncheck the Enbloc Dialing check box, click <strong>Apply Config</strong>, and click <strong>Save</strong>. |
| Enhanced Secure Extension Mobility Cross Cluster | 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).                                                                                      | For more information, see <em>Cisco Unified Communications Manager Features and Services Guide</em>.               |</p>
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Configuration reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fast Dial Service</td>
<td>Allows a user to enter a Fast Dial code to place a call. Fast Dial codes can be assigned to phone numbers or Personal Address Book entries. (See Services in this table.)</td>
<td>For more information, see:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <em>Cisco Unified Communications Manager Administration Guide,</em> &quot;Cisco Unified IP Phone Configuration&quot; chapter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <em>Cisco Unified Communications Manager System Guide,</em> &quot;Cisco Unified IP Phone Services&quot; chapter</td>
</tr>
<tr>
<td>Forced Authorization Codes (FAC)</td>
<td>Controls the types of calls that certain users can place.</td>
<td>For more information, see the <em>Cisco Unified Communications Manager Features and Services Guide,</em> &quot;Client Matter Codes and Forced Authorization Codes&quot; chapter.</td>
</tr>
<tr>
<td>(SCCP phones only)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Group Call Pickup</td>
<td>Allows a user to answer a call that is ringing on a directory number in another group.</td>
<td>For more information, see the <em>Cisco Unified Communications Manager Features and Services Guide,</em> &quot;Call Pickup&quot; chapter.</td>
</tr>
<tr>
<td>Hardware Updates</td>
<td>Improves the compatibility of internal phone components. Phone models manufactured with the following hardware versions must run Firmware Release 9.3(1) SR1 or later. The phone firmware does not allow the phone to be downgraded to releases earlier than Release 9.3(1) SR1.</td>
<td>No configuration required</td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified Wireless IP Phone 7945G with hardware versions 13.0 and higher.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified Wireless IP Phone 7965G with hardware versions 13.0 and higher.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified Wireless IP Phone 7975G with hardware versions 12.0 and higher.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The hardware version is found on the Device Information web page for the phone.</td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Configuration reference</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Headset Sidetone Control and Send Gain</td>
<td>Allows an administrator to set the sidetone level and send gain level of a wired headset.</td>
<td>For more information, see the <em>Cisco Unified Communications Manager Features and Services Guide</em>, “Cisco Unified IP Phone Configuration” chapter.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The sidetone and send gain levels are applicable only to Cisco Unified IP Phones 7945, 7965, and 7975.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Available sidetone levels are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Off</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Lowest</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Default</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Low</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Mid</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Mid-High</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• High</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Higher</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Highest</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Available send gain levels are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Lowest</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Lower</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Default</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• High</td>
<td></td>
</tr>
<tr>
<td>Help system</td>
<td>Provides a comprehensive set of topics that appear on the phone screen.</td>
<td>No configuration required.</td>
</tr>
<tr>
<td>Hold/Resume</td>
<td>Allows the user to move a connected call between an active state and a held state.</td>
<td>Requires no configuration, unless you want to use Music on Hold. See the “Music on Hold” entry in this table for more information. Also, see the “Hold Reversion” entry in this table.</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Configuration reference</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Hold Reversion</td>
<td>Limits the amount of time that a call can be on hold before reverting back to the phone that put the call on hold and alerting the user. Reverting calls are distinguished from incoming calls by a single ring (or beep, depending on the new call indicator setting for the line). This notification repeats at intervals if not resumed. A call that triggers Hold Reversion also displays an animated icon in the call bubble and a brief message on the status line. You can configure call focus priority to favor incoming or reverting calls.</td>
<td>For more information, see the <em>Cisco Unified Communications Manager Features and Services Guide</em>, “Hold Reversion” chapter.</td>
</tr>
<tr>
<td>Hold Status</td>
<td>Enables phones with a shared line to distinguish between the local and remote lines that placed a call on hold.</td>
<td>No configuration required.</td>
</tr>
<tr>
<td>Hunt Group Display</td>
<td>Provides load sharing for calls to a main directory number. A hunt group contains a series of directory numbers that can answer the incoming calls. When an incoming call is offered to a directory number that is part of the hunt group, this feature displays the main directory number in addition to the calling party.</td>
<td>For more information, see:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <em>Cisco Unified Communications Manager Administration Guide</em>, “Hunt Group Configuration” chapter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <em>Cisco Unified Communications Manager System Guide</em>, “Understanding Route Plans” chapter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <em>Cisco Unified Communications Manager Administration Guide</em>, “CTI Route Point Configuration” chapter</td>
</tr>
<tr>
<td>Immediate Divert</td>
<td>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.</td>
<td>For more information, see the <em>Cisco Unified Communications Manager System Guide</em>, “Cisco Unified IP Phones” chapter.</td>
</tr>
<tr>
<td>Immediate Divert—Enhanced</td>
<td>Allows users to transfer incoming calls directly to their voice messaging system or to the voice messaging system of the original called party.</td>
<td>For more information, see the <em>Cisco Unified Communications Manager System Guide</em>, “Cisco Unified IP Phones” chapter.</td>
</tr>
<tr>
<td>Intelligent Session Control</td>
<td>Reroutes a direct call to a user mobile phone to the enterprise number (desk phone). For an incoming call to a remote destination (mobile phone), only the remote destination rings; the desk phone does not ring. When the call is answered on the mobile phone, the desk phone displays a Remote in Use message. During these calls, a user can use the various features of the mobile phone.</td>
<td>For more information, see the <em>Cisco Unified Communications Manager Features and Services Guide</em>, “Cisco Unified Mobility” chapter.</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Configuration reference</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Intercom        | Allows users to place and receive intercom calls using programmable phone buttons. You can configure intercom line buttons to:  
• Directly dial a specific intercom extension.  
• Initiate an intercom call and then prompt the user to enter a valid intercom number.  
**Note** If a user logs into the same phone on a daily basis using their Cisco Extension Mobility profile, assign the phone button template that contains intercom information to their profile, and assign the phone as the default intercom device for the intercom line. | For more information, see the *Cisco Unified Communications Manager Feature and Services Guide*, “Intercom” chapter. |
| Join/Select     | Creates a conference by joining together existing calls that are on a single phone line.       | For more information, see the *Cisco Unified IP Phone 7975G, 7971G-GE, 7970G, 7965G, and 7945G User Guide for Cisco Unified Communications Manager (SCCP and SIP)*, “Calling Features” chapter, “Making Conference Calls” section. |
| Join Across Lines/Select | Allows users to apply the Join feature to calls that are on multiple phone lines.          | For more information, see:  
• *Softkey Templates*, on page 155  
• *Cisco Unified Communications Manager System Guide*, “Cisco Unified IP Phones” chapter |
| Line Select     | If this feature is disabled (default), then the ringing line is selected. When enabled, the primary line is picked up even if a call is ringing on another line. The user must manually select the other line.  
**Note** This feature can also be enabled or disabled for Extension Mobility. | For more information, see the “Always use prime line” option in the following chapters of *Cisco Unified Communications Manager Administration Guide*:  
• Device Profile Configuration  
• Common Phone Profile Configuration  
• Cisco Unified IP Phone Configuration |
<p>| Feature                          | Description                                                                                                                                                                                                 | Configuration reference                                                                                                                                                                                                 | Line Select for Voice Messages                                                                                                                                                                                                                       |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------| For more information, see the &quot;Always use prime line option for voice message&quot; in the following chapters of Cisco Unified Communications Manager Administration Guide:                                                                                           |
|                                | When disabled (default), pressing the Messages button selects the line that has a voice message. If more than one line has voice mail, then the first available line is selected. When enabled, the primary line is always used to retrieve voice messages. | • Device Profile Configuration                                                                                                                                  • Common Phone Profile Configuration                                                                                                                    • Cisco Unified IP Phone Configuration                                                                                                                                                           |
|                                | Note: This feature can also be enabled or disabled for Extension Mobility.                                                                                                                                  |                                                                                                                                                                                                                           | For more information, see the &quot;Line Select for Voice Messages&quot; in the following chapters of Cisco Unified Communications Manager Administration Guide:                                                                                           |
| 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 non-hunt group calls from ringing their phone. | For more information, see:                                                                                                                                  • Softkey Templates, on page 155                                                                                                                                  • Cisco Unified Communications Manager System Guide, &quot;Understanding Route Plans” chapter                                                                                               |
| Malicious Call Identification (MCID) | Allows users to notify the system administrator about suspicious calls that are received.                                                                                                                      | For more information, see:                                                                                                                                                                                                      • Cisco Unified Communications Manager System Guide, &quot;Cisco Unified IP Phones” chapter                                                                                          |
|                                |                                                                                                                                                                                                            | • Cisco Unified Communications Manager Features and Services Guide, &quot;Malicious Call Identification” chapter                                                                                                                |                                                                                                                                                                                                                                                      |
| Meet Me Conference              | Allows a user to host a Meet Me conference in which other participants call a predetermined number at a scheduled time.                                                                                       | For more information, see the Cisco Unified Communications Manager Administration Guide, &quot;Meet-Me Number/Pattern Configuration” chapter.                                                                                                                |                                                                                                                                                                                                                                                      |
| Message Waiting                 | Defines directory numbers for message-waiting on and message-waiting off indicator. A directly connected voice-messaging system uses the specified directory number to set or to clear a message-waiting indication for a particular Cisco Unified IP Phone. | For more information, see:                                                                                                                                                                                                      • Cisco Unified Communications Manager Administration Guide, &quot;Message Waiting Configuration&quot; chapter                                                                                          |
|                                |                                                                                                                                                                                                            | • Cisco Unified Communications Manager System Guide, &quot;Voice Mail Connectivity to Cisco Unified Communications Manager” chapter                                                                                                             |                                                                                                                                                                                                                                                      |</p>
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Configuration reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message Waiting Indicator</td>
<td>A light on the handset that indicates that a user has one or more new voice messages.</td>
<td>For more information, see:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <em>Cisco Unified Communications Manager Administration Guide</em>, “Message Waiting Configuration” chapter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <em>Cisco Unified Communications Manager System Guide</em>, “Voice Mail Connectivity to Cisco Unified Communications Manager” chapter</td>
</tr>
<tr>
<td>Missed Call Logging</td>
<td>Allows a user to specify whether missed calls will be logged in the missed calls directory for a given line appearance.</td>
<td>For more information, see the <em>Cisco Unified Communications Manager Administration Guide</em>, “Directory Number Configuration” chapter.</td>
</tr>
<tr>
<td>Mobile Connect</td>
<td>Enables users to manage business calls using a single phone number and pick up in-progress calls on the desktop phone and mobile phone. Users can restrict the group of callers according to phone number and time of day.</td>
<td>For more information, see the <em>Cisco Unified Communications Manager Features and Services Guide</em>, “Cisco Unified Mobility” chapter.</td>
</tr>
<tr>
<td>Mobile Voice Access</td>
<td>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 mobile phone.</td>
<td>For more information, see the <em>Cisco Unified Communications Manager Features and Services Guide</em>, “Cisco Unified Mobility” chapter.</td>
</tr>
<tr>
<td>Multilevel Precedence and Preemption (MLPP) (SCCP phones only)</td>
<td>Provides a method of prioritizing calls within your phone system. Use this feature when users work in an environment where they need to make and receive urgent or critical calls.</td>
<td>For more information, see the <em>Cisco Unified Communications Manager Features and Services Guide</em>, “Multilevel Precedence and Preemption” chapter.</td>
</tr>
<tr>
<td>Multiple calls per line appearance</td>
<td>Each line can support multiple calls. Only one call can be active at any time; other calls are automatically placed on hold.</td>
<td>For more information, see the <em>Cisco Unified Communications Manager Administration Guide</em>, “Directory Number Configuration” chapter.</td>
</tr>
<tr>
<td>Music On Hold</td>
<td>Plays music while callers are on hold.</td>
<td>For more information, see the <em>Cisco Unified Communications Manager Features and Services Guide</em>, “Music On Hold” chapter.</td>
</tr>
<tr>
<td>Mute</td>
<td>Mutes the microphone from the handset or headset.</td>
<td>No configuration required.</td>
</tr>
<tr>
<td>Onhook Call Transfer</td>
<td>Allows a user to press a single Transfer softkey and then go onhook to complete a call transfer.</td>
<td>For more information, see the <em>Cisco Unified Communications Manager System Guide</em>, “Cisco Unified IP Phones” chapter.</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Configuration reference</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Onhook Predialing</td>
<td>Allows a user to dial a number without going off hook. The user can then either pick up the handset or press the Dial softkey.</td>
<td>For more information, see the <em>Cisco Unified IP Phone 7975G, 7971G-GE, 7970G, 7965G, and 7945G User Guide for Cisco Unified Communications Manager (SCCP and SIP)</em>, “Basic Call Handling” chapter.</td>
</tr>
<tr>
<td>Other Group Pickup</td>
<td>Allows a user to answer a call ringing on a phone in another group that is associated with the user group.</td>
<td>For more information, see the <em>Cisco Unified Communications Manager Features and Services Guide</em>, “Call Pickup” chapter.</td>
</tr>
<tr>
<td>Phone Screen Illumination Disabling (Cisco Unified IP Phone 7965G and 7945G only)</td>
<td>Allows user to disable phone screen illumination on a phone, which would override other rules that determine when the phone screen gets illuminated. To provide this feature, you must implement the Display URI, which includes configuring the length of time that illumination remains disabled.</td>
<td>For more information, see the <em>Cisco Unified IP Phone Service Application Development Notes</em> at the following location: <a href="http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_programming_reference_guides_list.html">http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_programming_reference_guides_list.html</a></td>
</tr>
<tr>
<td>Phone Secure Web Access</td>
<td>Cisco Unified IP Phones can now securely access the web with the use of a phone trust store called “phone-trust.”</td>
<td>For more information, see the <em>Cisco Unified Communications Manager Security Guide</em>, “Security Overview” chapter.</td>
</tr>
<tr>
<td>Plus Dialing</td>
<td>Allows the user to dial E.164 numbers prefixed with a “+” sign. To dial the + sign, the user needs to press and hold the “*” key for at least 1 second. This applies to dialing the first digit for an on-hook or off-hook call only.</td>
<td>No configuration required</td>
</tr>
<tr>
<td>Presence-Enabled directories</td>
<td>Allows a user to monitor the call state of another directory number (DN) listed in call logs, speed dials, and corporate directories. The Busy Lamp Field (BLF) for the DN displays the call state.</td>
<td>For more information, see the <em>Cisco Unified Communications Manager Features and Services Guide</em>, “Presence” chapter.</td>
</tr>
<tr>
<td>Private Line Automated Ringdown (PLAR)</td>
<td>The Cisco Unified Communications Manager administrator can configure a phone number that the Cisco Unified IP Phone dials as soon as the handset goes off hook. This can be useful for phones that are designated for calling emergency or “hotline” numbers.</td>
<td>For more information on SIP, see the <em>Cisco Unified Communications Manager System Guide</em>, “SIP Dial Rules Configuration” chapter. For more information on SCCP, see the <em>Cisco Unified Communications Manager Administration Guide</em>, “Directory Number Configuration” chapter, “Configuring PLAR” section.</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Configuration reference</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Privacy</td>
<td>Prevents users who share a line from adding themselves to a call and from viewing information on their phone screens about the call of the other user.</td>
<td>For more information, see:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <em>Cisco Unified Communications Manager Administration Guide</em>, &quot;Cisco Unified IP Phone Configuration&quot; chapter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <em>Cisco Unified Communications Manager System Guide</em>, &quot;Cisco Unified IP Phones&quot; chapter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <em>Cisco Unified Communications Manager Features and Services Guide</em>, &quot;Barge and Privacy&quot; chapter</td>
</tr>
<tr>
<td>Programmable Line Keys</td>
<td>The administrator can assign features to line buttons. Softkeys normally control these features; for example, New Call, Call Back, End Call, and Forward All. When the administrator configures these features on the line buttons, they always remain visible, so users can have a &quot;hard&quot; New Call key.</td>
<td>For more information, see:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <em>Cisco Unified Communications Manager System Guide</em>, &quot;Cisco Unified IP Phone&quot; chapter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <em>Cisco Unified Communications Manager Administration Guide</em>, &quot;Phone Button Template Configuration&quot; chapter</td>
</tr>
<tr>
<td>Protected Calling</td>
<td>Provides a secure (encrypted) connection between two phones. A security tone is played at the beginning of the call to indicate that both phones are protected. Some features, such as conference calling, shared lines, Extension Mobility, and Join Across Lines are not available when protected calling is configured. Protected calls are not authenticated.</td>
<td>For more information about security, see <em>Supported Security Features</em>, on page 15.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For additional information, see the <em>Cisco Unified Communications Manager Security Guide</em>, &quot;Configuring a Phone Security Profile&quot; chapter.</td>
</tr>
<tr>
<td>Quality Reporting Tool (QRT)</td>
<td>Allows users to use the QRT softkey on a phone to submit information about problem phone calls. QRT can be configured for either of two user modes, depending upon the amount of user interaction desired with QRT.</td>
<td>For more information, see:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <em>Cisco Unified Communications Manager System Guide</em>, &quot;Cisco Unified IP Phones&quot; chapter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <em>Cisco Unified Communications Manager Features and Services Guide</em>, &quot;Quality Report Tool&quot; chapter</td>
</tr>
<tr>
<td>Redial</td>
<td>Allows users to call the most recently dialed phone number by pressing a softkey.</td>
<td>No configuration required.</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Configuration reference</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Remote Port Configuration    | Allows the administrator to configure the speed and duplex function of the phone Ethernet ports remotely by using Cisco Unified Communications Manager Administration. This enhances the performance for large deployments with specific port settings.  
**Note**  
If the ports are configured for Remote Port Configuration in Cisco Unified Communications Manager, the data cannot be changed on the phone. | To configure the parameter in the Cisco Unified Communications Manager Administration application, choose Device > Phone, select the appropriate IP phones, and scroll to the Product Specific Configuration Layout pane (Switch Port Remote Configuration or PC Port Remote Configuration).  
To configure the setting on multiple phones simultaneously, configure the Remote Port Configuration in the Enterprise Phone Configuration (System > Enterprise Phone Configuration).  
For more information, see:  
• *Cisco Unified Communications Manager Administration Guide,* "Directory Number Configuration" chapter  
• *Custom Phone Ring Creation,* on page 168 |
| Ring Setting                 | Identifies ring type used for a line when a phone has another active call.                       | For more information, see:  
• *Cisco Unified Communications Manager Administration Guide,* "Directory Number Configuration" chapter  
• *Custom Phone Ring Creation,* on page 168                                                                                                                                                                                                                                                                                                                                                                                                 |
| Ringer Volume Control        | The Ringer Volume Control feature enables the system administrator to control the minimum ringer-volume setting and adjust the minimum volume level for the ringer. Individual users cannot make the changes to the minimum ringer-volume setting.  
When a user presses the minus (–) side of the Volume button to reduce the ringer volume in an on-hook state, the volume decreases only to the configured minimum volume-level setting. When the minimum volume level is reached, no status message appears.  
After a system restart, the minimum ringer volume resets to the minimum ringer-volume setting that is received from the configuration file. If the system administrator configured a new minimum volume level since the last startup and the end user had previously set the minimum ringer volume lower, the ringer volume will be set to the minimum value from the configuration file, not to the user setting.  
This feature does not apply to handset, speaker, and headset volumes during calls. | To configure the parameter in the Cisco Unified Communications Manager Administration application, choose Device > Phone, select the appropriate IP phones, and scroll to the Product Specific Configuration Layout pane.  
For more information, see:  
• *Cisco Unified Communications Manager Administration Guide,* "Directory Number Configuration" chapter  
• *Custom Phone Ring Creation,* on page 168 |
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Configuration reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>RTCP Hold For SIP</td>
<td>The RTCP Hold For SIP feature 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. Enable the RTCP option on the Cisco Unified Communications Manager to support this feature.</td>
<td>No configuration required.</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Configuration reference</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Secure and Nonsecure</td>
<td>When a phone is configured as secure (encrypted and trusted) in Cisco Unified Communications Manager, it can be given a protected status. Afterward, the protected phone can be configured to play an indication tone at the beginning of a call:</td>
<td>No configuration required.</td>
</tr>
<tr>
<td>Indication Tone</td>
<td>• Protected Device: To change the status of a secure phone to protected, check the &quot;Protected Device&quot; check box in Cisco Unified Communications Manager Administration (Device &gt; Phone &gt; Phone Configuration).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Play Secure Indication Tone: To enable the protected phone to play a secure or nonsecure indication tone, set the &quot;Play Secure Indication Tone&quot; to True. (The default is False.) You set this option in Cisco Unified Communications Manager Administration (System &gt; Service Parameters). Select the server and then the Cisco CallManager service. In the Service Parameter Configuration window, select the option in the Feature - Secure Tone area. (The default is False.)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Only protected phones hear these secure or nonsecure indication tones. (Nonprotected phones never hear tones.) If the overall call status changes during the call, the indication tone changes accordingly. At that time, the protected phone plays the appropriate tone.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>A protected phone plays a tone or not under these circumstances:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• When the option to play the tone is enabled Play Secure Indication Tone option is enabled (True):</td>
<td></td>
</tr>
<tr>
<td></td>
<td>◦ When end-to-end secure media is established and the call status is secure, the phone plays the secure indication tone (three long beeps with pauses).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>◦ When end-to-end nonsecure media is established and the call status is nonsecure, the phone plays the nonsecure indication tone (six short beeps with brief pauses).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If the Play Secure Indication Tone option is disabled, no tone plays.</td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Configuration reference</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>Secure Extension Mobility Cross Cluster</td>
<td>Secure Extension Mobility Cross Cluster (EMCC) feature enables a user configured in one cluster to log into a Cisco Unified IP Phone in another cluster. The users from a home cluster log into a Cisco Unified IP Phone at a visiting cluster. The visiting cluster fails to log into home cluster in secure mode.</td>
<td>For more information, see <a href="https://www.cisco.com/c/en/us/products/unified-communications/unified-communications-manager-unified-cm/quick-ref-guide.html">Cisco Unified Communications Manager Features and Services Guide</a>, &quot;Cisco Extension Mobility Cross Cluster&quot; chapter.</td>
</tr>
</tbody>
</table>
| Secure Conference | Allows secure phones to place conference calls by using a secured conference bridge. As new participants are added by using Confrn, Join, cBarge, Barge softkeys or Meet-Me conferencing, the secure call icon displays as long as all participants use secure phones. 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 Advance Adhoc Conference parameter is set. | For more information about security, see [Supported Security Features](https://www.cisco.com/c/en/us/products/unified-communications/unified-communications-manager-unified-cm-security-kit/quick-ref-guide.html), on page 15. For more information, see:  
| Security Hardening | Improves the phone firmware security. | No configuration required. |
| Services | Allows you to use the Cisco Unified IP Phone Services Configuration menu in Cisco Unified Communications Manager Administration to define and maintain the list of phone services to which users can subscribe. | For more information, see:  
| Services URL Button | Allows users to access services from a programmable button rather than by using the Services menu on a phone. | For more information, see:  
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Configuration reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Handoff</td>
<td>Allows users to switch calls from a mobile phone to Cisco Unified devices that share the same line. Handsets on all the devices on the shared line then flash simultaneously. After a user answers the call from one of the CiscoUnified devices, the other Cisco Unified devices that share the same line display a Remote in Use message. However, if the call fails to switch from the mobile phone, the mobile phone might display a Cannot Move Conversation message.</td>
<td>For more information, see the <em>Cisco Unified Communications Manager Features and Services Guide</em>, &quot;Cisco Unified Mobility&quot; and &quot;Cisco Unified Mobility Advantage and Cisco Unified Mobile Communicator Integration&quot; chapters.</td>
</tr>
<tr>
<td>Shared Line</td>
<td>Allows a user to have several phones that share the same phone number or allows a user to share a phone number with a coworker.</td>
<td>For more information, see the <em>Cisco Unified Communications Manager System Guide</em>, &quot;Directory Number Configuration&quot; chapter.</td>
</tr>
<tr>
<td>Silent Monitoring</td>
<td>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. When a call is secured, the security status of the call is displayed as a lock icon on Cisco Unified IP Phones. The connected parties might also hear an audible alert tone that indicates the call is secured and is being monitored. <strong>Note</strong> When an active call is being monitored or recorded, you can receive or place intercom calls; however, if you 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.</td>
<td>For more information, see the <em>Cisco Unified Communications Manager Features and Services Guide</em>, &quot;Monitoring and Recording&quot; chapter.</td>
</tr>
<tr>
<td>Single Button Barge</td>
<td>Allows users to press a line key to Barge or eBarge into a remote-in-use call on a shared line.</td>
<td>For more information, see:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <em>Cisco Unified Communications Manager Administration Guide</em>, &quot;Device Pool Configuration&quot; chapter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <em>Cisco Unified Communications Manager System Guide</em>, &quot;Cisco Unified IP Phones&quot; chapter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <em>Cisco Unified Communications Manager Features and Services Guide</em>, &quot;Barge and Privacy&quot; chapter</td>
</tr>
<tr>
<td>SIP Phone No Alert Name</td>
<td>Identifies the original source of a transferred call. The call appears on the call display as an Alert Call followed by the original caller telephone number.</td>
<td>No configuration required.</td>
</tr>
</tbody>
</table>

For more information, see:

- *Cisco Unified Communications Manager Administration Guide*, "Device Pool Configuration" chapter
- *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones" chapter
- *Cisco Unified Communications Manager Features and Services Guide*, "Barge and Privacy" chapter
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Configuration reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Speed Dialing</td>
<td>Dials a specified number that has been previously stored.</td>
<td>For more information, see:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <em>Cisco Unified Communications Manager Administration Guide</em>, &quot;Cisco Unified IP Phone Configuration&quot; chapter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <em>Cisco Unified Communications Manager System Guide</em>, &quot;Cisco Unified IP Phones&quot; chapter</td>
</tr>
<tr>
<td>SSH Access</td>
<td>Allows the administrator to enable or disable the SSH Access setting by using the Cisco Unified Communications Manager Administration application. This option indicates whether the phone supports the SSH Access. Settings include: • Enabled • Disabled (default)</td>
<td>To configure the parameter in the Cisco Unified Communications Manager Administration application, choose <strong>Device &gt; Phone</strong>, select the appropriate IP Phones, scroll to the <strong>Product Specific Configuration Layout</strong> area and select <strong>Enable</strong> from the <strong>SSH Access</strong> drop-down list box. If you set the same parameter in the Common Phone Profile window (<strong>Device &gt; Device Settings &gt; Common Phone Profile</strong>), the precedence order of the settings is: 1 Phone Configuration window settings 2 Common Phone Profile window settings</td>
</tr>
<tr>
<td>Time-of-Day Routing</td>
<td>Restricts access to specified telephony features by time period.</td>
<td>For more information, see:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <em>Cisco Unified Communications Manager Administration Guide</em>, “Time Period Configuration” chapter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <em>Cisco Unified Communications Manager System Guide</em>, “Time-of-Day Routing” chapter</td>
</tr>
<tr>
<td>Time Zone Update</td>
<td>Updates the Cisco Unified IP Phone with time zone changes.</td>
<td>For more information, see the <em>Cisco Unified Communications Manager Administration Guide</em>, &quot;Date/Time Group Configuration&quot; chapter.</td>
</tr>
<tr>
<td>Touchscreen Illumination Disabling  (Cisco Unified IP Phone 7975G, 7971G-GE, and 7970G only)</td>
<td>Allows user to disable touchscreen illumination on a phone, which would override other rules that determine when the touchscreen gets illuminated. To provide this feature, you must implement the Display URI, which includes configuring the length of time that illumination remains disabled.</td>
<td>For more information, see the <em>Cisco Unified IP Phone Service Application Development Notes</em> at the following location: <a href="http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_programming_reference_guides_list.html">http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_programming_reference_guides_list.html</a></td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Configuration reference</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>UCR 2008</td>
<td>The IP phones that use SCCP support Unified Capabilities Requirements (UCR) 2008 by providing the following functions:</td>
<td>For more information, see UCR 2008 Setup, on page 162.</td>
</tr>
<tr>
<td></td>
<td>• Support for Federal Information Processing Standard (FIPS) 104-2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Support for TVS IPv6</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Support for 80-bit SRTCP Tagging</td>
<td></td>
</tr>
<tr>
<td></td>
<td>As an IP Phone administrator, some of these functions require you to set up specific parameters in Cisco Unified Communications Manager Administration.</td>
<td></td>
</tr>
<tr>
<td>Video Mode</td>
<td>Allows a user to select the video display mode for viewing a video conference, depending on the modes configured in the system.</td>
<td>For more information, see:</td>
</tr>
<tr>
<td>(SCCP phones only)</td>
<td></td>
<td>• Cisco Unified Communications Manager Administration Guide, “Conference Bridge Configuration” chapter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cisco Unified Communications Manager System Guide, &quot;Understanding Video Telephony&quot; chapter</td>
</tr>
<tr>
<td>Video Support</td>
<td>Enables video support on the phone.</td>
<td>For more information, see:</td>
</tr>
<tr>
<td>(SCCP phones only)</td>
<td></td>
<td>• Cisco Unified Communications Manager Administration Guide, &quot;Conference Bridge Configuration&quot; chapter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cisco Unified Communications Manager System Guide, &quot;Understanding Video Telephony&quot; chapter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cisco VT Advantage Administration Guide, &quot;Overview of Cisco VT Advantage&quot; chapter</td>
</tr>
<tr>
<td>Voice Messaging System</td>
<td>Enables callers to leave messages if calls are unanswered.</td>
<td>For more information, see:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cisco Unified Communications Manager Administration Guide, &quot;Cisco Voice-Mail Port Configuration” chapter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cisco Unified Communications Manager System Guide, “Voice Mail Connectivity to Cisco Unified Communications Manager” chapter</td>
</tr>
</tbody>
</table>
VPN Client
(Cisco Unified IP Phone 7945G, 7965G, and 7975G only)

Provides a VPN connection using SSL on Cisco Unified IP Phone 7945G, 7965G, and 7975G for situations in which a phone is located outside a trusted network or when network traffic between the phone and Cisco Unified Communications Manager must cross untrusted networks.

For more information, see Cisco Unified Communications Manager Security Guide, "Virtual Private Network Configurations" chapter.

Product-Specific Parameters

Cisco Unified Communications Manager Administration allows you to set some product specific configuration parameters for Cisco Unified IP Phones. The following table lists the configuration windows and path in Cisco Unified Communications Manager Administration.

Table 38: Configuration Windows for Cisco Unified IP Phone

<table>
<thead>
<tr>
<th>Configuration window</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise Phone Configuration window</td>
<td>System &gt; Enterprise Phone Configuration</td>
</tr>
<tr>
<td>Common Phone Profile window</td>
<td>Device &gt; Device Settings &gt; Common Phone Profile</td>
</tr>
<tr>
<td>Phone Configuration window</td>
<td>Device &gt; Phone; Product Specific Configuration area of window</td>
</tr>
</tbody>
</table>

You can set the following parameters in any of the three configuration windows:

- Settings Access
- Video Capabilities
- Web Access
- Load Server
- RTCP
- Peer Firmware Sharing
- Cisco Discovery Protocol (CDP): Switch Port
- Cisco Discovery Protocol (CDP): PC Port
- Link Layer Discovery Protocol - Media Endpoint Discover (LLDP-MED): Switch Port
- Link Layer Discovery Protocol (LLDP): PC Port
- IPv6 Load Server
- 802.1x Authentication
- Switch Port Remote Configuration
• PC Port Remote Configuration
• Automatic Port Synchronization
• SSH Access

When you set the parameters, select the Override Common Settings check box for each setting you wish to update. If you do not check this box, the corresponding parameter setting does not take effect. If you set the parameters at the three configuration windows, the setting takes precedence in the following order:

• Phone Configuration window (highest precedence)
• Common Phone Profile Configuration window
• Enterprise Phone Configuration window (lowest precedence)

Corporate and Personal Directories

The **Directories** button on the Cisco Unified IP Phones gives users access to several directories. These directories can include:

- **Corporate Directory**: Allows a user to look up phone numbers for coworkers.
  
  To support this feature, you must configure corporate directories.

- **Personal Directory**: Allows a user to store a set of personal numbers.
  
  To support this feature, you must provide the user with software to configure the personal directory.

Corporate Directory Setup

Cisco Unified Communications Manager uses a Lightweight Directory Access Protocol (LDAP) directory to store authentication and authorization information about users of Cisco Unified Communications Manager applications that interface with Cisco Unified Communications Manager. Authentication establishes a user right to access the system. Authorization identifies the telephony resources that a user is permitted to use, such as a specific telephone extension.

For more information on directories, see the *Cisco Unified Communications Manager System Guide*, “Understanding Directory” chapter.

To install and set up these features, see the *Cisco Unified Communications Manager Administration Guide*, “LDAP System Configuration”, “LDAP Directory Configuration”, and “LDAP Authentication Configuration” chapters.

After completing the LDAP directory configuration, users can use the Corporate Directory service on their Cisco Unified IP Phone to look up users in the corporate directory.

Personal Directory Setup

Personal Directory consists of the following features:

- **Personal Address Book (PAB)**
- **Personal Fast Dials (Fast Dials)**
Address Book Synchronization Tool (TABSsync)

Users can access Personal Directory features by these methods:

• From a web browser: Users can access the PAB and Fast Dials features from the Cisco Unified Communications Manager User Options web pages.

• From the Cisco Unified IP Phone: Users can choose Directories > Personal Directory to access the PAB and Fast Dials features from their phones.

• From a Microsoft Windows application: Users can use the TABSync tool to synchronize their PABs with Microsoft Windows Address Book (WAB). Customers who want to use the Microsoft Outlook Address Book (OAB) should begin by importing the data from the OAB into the Windows Address Book (WAB). TabSync can then be used to synchronize the WAB with Personal Directory.

To ensure that Cisco Unified IP Phone Address Book Synchronizer users have access only to end user data that pertains to them, activate the Cisco UXL Web Service in Cisco Unified Serviceability.

To configure Personal Directory from a web browser, users must access their User Options web pages. You must provide users with a URL and login information.

To synchronize with Microsoft Outlook, users must install the TABSync utility, which you provide. For more information, see Obtain Cisco Unified IP Phone Address Book Synchronizer, on page 246 and Cisco Unified IP Phone Address Book Synchronizer Deployment, on page 247.

Phone Button Templates

Phone button templates let you assign speed dials and call-handling features to programmable line buttons. Call-handling features that can be assigned to buttons include call forward, hold, and conference.

Ideally, you modify templates before registering phones on the network. In this way, you can access customized phone button template options from Cisco Unified Communications Manager during registration.

To modify a phone button template, choose Device > Device Settings > Phone Button Template from Cisco Unified Communications Manager Administration. To assign a phone button template to a phone, use the Phone Button Template field in the Cisco Unified Communications Manager Administration Phone Configuration window. For more information, see the Cisco Unified Communications Manager Administration Guide and the Cisco Unified Communications Manager System Guide.

Cisco Unified IP Phone 7975G, 7971G-GE, and 7970G Phone Button Templates

The default template that ships with the Cisco Unified IP Phone 7975G, 7971G-GE, and 7970G uses buttons 1 and 2 for lines and assigns buttons 3 through 8 as speed dial.

The recommended standard Cisco Unified IP Phone 7970 Series template uses buttons 1 and 2 for lines, assigns buttons 3 through 5 as speed dial, and buttons 6 through 8 as Hold, Conference, and Transfer, respectively.

To avoid confusion for users, do not assign a feature to a button and a softkey at the same time.
Cisco Unified IP Phone 7965G Phone Button Templates

The default Cisco Unified IP Phone 7965G template that ships with the phone uses buttons 1 and 2 for lines and assigns buttons 3 through 6 as speed dial.

The recommended standard Cisco Unified IP Phone 7965G template uses buttons 1 and 2 for lines, assigns button 3 as speed dial, and buttons 4 through 6 as Hold, Conference, and Transfer, respectively.

To avoid confusion for users, do not assign a feature to a button and a softkey at the same time.

Cisco Unified IP Phone 7945G Phone Button Templates

The default Cisco Unified IP Phone 7945G template that ships with the phone uses buttons 1 and 2 for lines.

The recommended standard Cisco Unified IP Phone 7945G template uses buttons 1 and 2 for lines.

To avoid confusion for users, do not assign a feature to a button and a softkey at the same time.

Phone Button Template for Personal Address Book or Fast Dials

To avoid confusion for users, do not assign a feature to a button and a softkey at the same time.

For additional information on IP phone services, see the Cisco Unified Communications Manager Administration Guide, "IP Phone Services Configuration" chapter. For more information on configuring line buttons, see the Cisco Unified Communications Manager Administration Guide, "Cisco Unified IP Phone Configuration" chapter.

Related Topics

Softkey Templates, on page 155

Set Up PAB or Fast Dial in IP Phone Services

To configure PAB or Fast Dial as an IP phone service, perform these steps:

Procedure

**Step 1** Choose Device > Device Settings > Phone Services. The Find and List IP Phone Services window displays.

**Step 2** Click Add New. The IP Phone Services Configuration window displays.

**Step 3** Enter the following settings:

- Service Name and ASCII Service Name: Enter Personal Address Book.
- Service Description: Enter an optional description of the service.
- Service URL

For PAB, enter the following URL:

http://<Unified CM-server-name>:8080/ccmpd/login.do?name=##DEVICENAME##&service=pab
For Fast Dial, enter the following URL:

http://<Unified-CM-server-name>:8080/ccmpd/login.do?name=#DEVICENAME#&service=fd

- Secure Service URL

For PAB, enter the following URL:

https://<Unified CM-server-name>:8443/ccmpd/login.do?name=#DEVICENAME#&service=pab

For Fast Dial, enter the following URL:

https://<Unified-CM-server-name>:8443/ccmpd/login.do?name=#DEVICENAME#&service=fd

- Service Category: Select XML Service.
- Service Type: Select Directories.
- Enable: Select the checkbox.

**Step 4**  Click **Save**.

You can add, update, or delete service parameters as needed as described in "IP Phone Service Parameter" chapter in the *Cisco Unified Communications Manager Administration Guide*.

**Note**  If you change the service URL, remove an IP phone service parameter, or change the name of a phone service parameter for a phone service to which users are subscribed, you must click **Update Subscriptions** to update all currently subscribed users with the changes, or users must resubscribe to the service to rebuild the correct URL.

---

**Change Phone Button Template for PAB or Fast Dial**

To modify a phone button template for PAB or Fast Dial, perform these steps:

**Procedure**

**Step 1**  From Cisco Unified Communications Manager Administration, choose **Device > Device Settings > Phone Button Template**.

**Step 2**  Click **Find**.

**Step 3**  Select the phone model.

**Step 4**  Click **Copy**, enter a name for the new template, and then click **Save**.

The Phone Button Template Configuration window opens.

**Step 5**  Identify the button you would like to assign, and select **Service URL** from the Features drop-down list box associated with the line.

**Step 6**  Click **Save** to create a new phone button template using the service URL.

**Step 7**  Choose **Device > Phone** and open the Phone Configuration window for the phone.

**Step 8**  Select the new phone button template from the Phone Button Template drop-down list box.

**Step 9**  Click **Save** to store the change and then click **Apply Config** to implement the change.

The phone user can now access the User Options pages and associate the service with a button on the phone.
For additional information on IP phone services, see the *Cisco Unified Communications Manager Administration Guide*, "IP Phone Services Configuration" chapter. For more information on configuring line buttons, see the *Cisco Unified Communications Manager Administration Guide*, “Cisco Unified IP Phone Configuration” chapter, “Configuring Speed-Dial Buttons” section.

## Softkey Templates

Using Cisco Unified Communications Manager Administration, you can manage softkeys associated with applications that are supported by the Cisco Unified IP Phone. Cisco Unified Communications Manager supports two types of softkey templates: standard and nonstandard. Standard softkey templates include Standard User, Standard Feature, Standard Assistant, Standard Manager, and Standard Shared Mode Manager. An application that supports softkeys can have one or more standard softkey templates associated with it. You can modify a standard softkey template by making a copy of it, giving it a new name, and making updates to that copied softkey template. You can also modify a nonstandard softkey template.

To configure softkey templates, choose **Device > Device Settings > Softkey Template** from Cisco Unified Communications Manager Administration. To assign a softkey template to a phone, use the Softkey Template field in the Cisco Unified Communications Manager Administration Phone Configuration window. For more information, see the *Cisco Unified Communications Manager Administration Guide* and the *Cisco Unified Communications Manager System Guide*.

---

**Note**
The Cisco Unified IP Phone 7975G, 7971G-GE, 7970G, 7965G, and 7945G supports all the softkeys that are configurable in Cisco Unified Communications Manager Administration.

## Services Setup

The **Services** button on the Cisco Unified IP Phone gives users access to Cisco Unified IP Phone Services. You can also assign services to the programmable buttons on the phone (see the Cisco Unified IP Phone User Guide for more information). These services comprise XML applications that enable the display of interactive content with text and graphics on the phone. Examples of services include local movie times, stock quotes, and weather reports.

Before a user can access any service:

- You must use Cisco Unified Communications Manager Administration to configure available services.
- The user must subscribe to services by using the Cisco Unified IP Phone User Options web pages. This web-based application provides a graphical user interface (GUI) for limited, end user configuration of IP Phone applications.

Before you set up services, gather the URLs for the sites that you want to set up and verify that users can access those sites from your corporate IP telephony network.

To set up these services, choose **Device > Device Settings > Phone Services** from Cisco Unified Communications Manager Administration. See the *Cisco Unified Communications Manager Administration Guide* and the *Cisco Unified Communications Manager System Guide* for more information.
After you configure these services, verify that your users have access to the Cisco Unified CM User Options web pages, from which they can select and subscribe to configured services. See Phone Features User Subscription and Setup, on page 245 for a summary of the information that you must provide to end users. Cisco Unified IP phones can support up to four HTTP/HTTPS active client connections and up to four HTTP/HTTPS active server connections at one time. A few examples of HTTP/HTTPS services include:

- Extension Mobility
- Directories
- Messages

Enable Device Invoked Recording

Configure the Device Invoked Recording feature from Cisco Unified Communications Manager Administration. For more information and detailed instructions, see the “Monitoring and Recording” chapter in the Cisco Unified Communications Manager Features and Services Guide.

Procedure

Step 1 Set the IP phone Built In Bridge to On.
Step 2 Set Recording Option to Selective Call Recording Enabled.
Step 3 Select the appropriate Recording Profile.

Cisco Unified Communications Manager User Addition

Adding users to Cisco Unified Communications Manager allows you to display and maintain information about users and allows each user to perform these tasks:

- Access the corporate directory and other customized directories from a Cisco Unified IP Phone.
- Create a personal directory.
- Set up Call Forwarding numbers.
- Subscribe to services that are accessible from a Cisco Unified IP Phone.

You can add users to Cisco Unified Communications Manager using either of these methods:

- To add users individually, choose User Management > End User from Cisco Unified Communications Manager Administration.

For more information on adding users, see the Cisco Unified Communications Manager Administration Guide. For details on user information, see the Cisco Unified Communications Manager System Guide.

- To add users in batches, use the Bulk Administration Tool. This method also enables you to set an identical default password for all users.

For more information, see the Cisco Unified Communications Manager Bulk Administration Guide.
To add users from your corporate LDAP directory, choose **System > LDAP > LDAP System** from Cisco Unified Communications Manager Administration.

**Note**

After the Enable Synchronization from LDAP Server is enabled, you will not be able to add additional users from Cisco Unified Communications Manager Administration.

For more information on LDAP, see the *Cisco Unified Communications Manager System Guide*, “Understanding the Directory”.

To add a user and a phone at the same time, choose **User Management > User/Phone Add** from Cisco Unified Communications Manager.

---

**User Options Web Page Management**

From the User Options web page, users can customize and control several phone features and settings. For more information about the User Options web pages, see the *Cisco Unified IP Phone 7975G, 7971G-GE, 7970G, 7965G, and 7945G User Guide for Cisco Unified Communications Manager (SCCP and SIP)*.

**User Access to User Options Web Pages**

Before a user can access the User Options web pages, you must add the user to the standard Cisco Unified Communications Manager end user group and associate the appropriate phone with the user.

Make sure to provide end users with the following information about the User Options web pages:

- The URL required to access the application. This URL is:
  
  \[http://<server_name:portnumber>/ccmuser/\], where `server_name` is the host on which the web server is installed.

- A user ID and default password are needed to access the application.

  These settings correspond to the values you entered when you added the user to Cisco Unified Communications Manager.

For more information, see:

- *Cisco Unified Communications Manager Administration Guide*, “User Group Configuration” and “End User Configuration” chapters
- *Cisco Unified Communications Manager System Guide*, “Roles and User Groups” chapter

**Related Topics**

- *Cisco Unified Communications Manager User Addition*, on page 156

**Add User to End User Group**

To add the user to the standard Cisco Unified Communications Manager End User group, perform these steps:
Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose User Management > User Groups. The Find and List Users window displays.

Step 2 Enter the appropriate search criteria and click Find.

Step 3 Click Standard CCM End Users. The User Group Configuration page for the Standard CCM End Users displays.

Step 4 Click Add End Users to Group. The Find and List Users window displays.

Step 5 Use the Find User drop-down list to find the end users that you want to add and click Find. A list of end users that matches your search criteria displays.

Step 6 In the list of records that displays, click the check box next to the users that you want to add to this user group. If the list comprises multiple pages, use the links at the bottom to see more results. Note The list of search results does not display end users that already belong to the user group.

Step 7 Click Add Selected.

Associate Phones with Users

To associate appropriate phones with the user, perform these steps:

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose User Management > End User. The Find and List Users window displays.

Step 2 Enter the appropriate search criteria and click Find.

Step 3 In the list of records that display, click the link for the user.

Step 4 Click Device Association. The User Device Association window displays.

Step 5 Enter the appropriate search criteria and click Find.

Step 6 Choose the device that you want to associate with the end user by checking the box to the left of the device.

Step 7 Click Save Selected/Changes to associate the device with the end user.

User Options Web Pages Options

Most options that are on the User Options web pages appear by default. However, the following options must be set by the system administrator using the Enterprise Parameters Configuration settings in Cisco Unified Communications Manager Administration:

- Show Ring Settings
Set Up User Options Web Page Options

To specify the options that appear on the User Options web pages, follow these steps:

**Procedure**

**Step 1**
From Cisco Unified Communications Manager Administration, choose **System > Enterprise Parameters**. The Enterprise Parameters Configuration window displays.

**Step 2**
In the CCMUser Parameters area, specify if a parameter appears on the User Options web pages by choosing one of these values from the **Parameter Value** drop-down list box for the parameter:

- **True**—Option displays on the User Options web pages (default).
- **False**—Option does not display on the User Options web pages.
- **Show All Settings**—All call forward settings display on the User Options web pages (default).
- **Hide All Settings**—No call forward settings display on the User Options web pages.
- **Show Only Call Forward All**—Only call forward all calls displays on the User Options web pages.

---

**EnergyWise Setup on Cisco Unified IP Phone**

To reduce power consumption, you can configure the phone to sleep (power down) and wake (power up) if your system includes an EnergyWise controller (for example, a Cisco Switch with the EnergyWise feature enabled).

You configure settings in Cisco Unified Communications Manager Administration to enable EnergyWise and configure sleep and wake times. These parameters are closely tied to the phone display configuration parameters.

When EnergyWise is enabled and a sleep time is set, the phone sends a request to the switch to wake it up at the configured time. The switch sends back either an acceptance or a rejection of the request. If the switch rejects the request or if the switch does not reply, the phone does not power down. If the switch accepts the request, the idle phone goes to sleep, reducing its power consumption to a predetermined level. A phone that is not idle sets an idle timer, and goes to sleep after the timer expires.

At the scheduled wake time, the system restores power to the phone, waking it up. To wake up the phone before the wake time, you must power on the phone from the switch. For more information, see the switch documentation.
The following table explains the Cisco Unified Communications Manager Administration fields that control the EnergyWise settings. You configure these fields in Cisco Unified Communications Manager Administration by choosing Device > Phone. You can also configure EnergyWise parameters in the Enterprise Phone Configuration and Common Phone Profile Configuration windows.

**Table 39: EnergyWise Configuration Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Power Save Plus</td>
<td>Selects the schedule of days for which the phone powers off. Select multiple days by pressing and holding the <strong>Control</strong> key while clicking on the days for the schedule. By default, no days are selected. When Enable Power Save is checked, you receive a message to warn about emergency (e911) concerns. <strong>Caution</strong> While Power Save Plus mode (hereafter, the mode) is in effect, endpoints configured for the mode are disabled for emergency calling and from receiving inbound calls. By selecting this mode, you agree to the following: (i) you are taking full responsibility for providing alternate methods for emergency calling and receiving calls while the mode is in effect; (ii) Cisco has no liability in connection with your selection of the mode and all liability in connection with enabling the mode is your responsibility; and (iii) you will inform users of the effects of the mode on calls, calling and otherwise. <strong>Note</strong> To disable Power Save Plus, you must uncheck the Allow EnergyWise Overrides checkbox. Leaving the Allow EnergyWise Overrides checked with no days selected in the Enable Power Save Plus field does not disable Power Save Plus.</td>
</tr>
<tr>
<td><strong>Phone On Time</strong></td>
<td>Determines when the phone automatically turns on for the days selected in the Enable Power Save Plus field. Enter the time in this field in 24 hour format, where 00:00 is midnight. For example, to automatically power up the phone at 7:00 a.m. (0700), enter 7:00. To power up the phone at 2:00 p.m. (1400), enter 14:00. The default value is blank, which means 00:00.</td>
</tr>
<tr>
<td><strong>Phone Off Time</strong></td>
<td>The time of day that the phone powers down for the days selected in the Enable Power Save Plus field. If the <strong>Phone On Time</strong> and the <strong>Phone Off Time</strong> fields contain the same value, the phone does not power down. Enter the time in this field in 24 hour format, where 00:00 is midnight. For example, to automatically power down the phone at 7:00 a.m. (0700), enter 7:00. To power down the phone at 2:00 p.m. (1400), enter 14:00. The default value is blank, which means 00:00.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Phone Off Idle Timeout</td>
<td>The length of time that the phone must be idle before the phone powers down. The range of the field is 20 to 1440 minutes. The default value is 60 minutes.</td>
</tr>
</tbody>
</table>
| Enable Audible Alert | When enabled, instructs the phone to play an audible alert starting at 10 minutes before to the time specified in the Phone Off Time field. The audible alert uses the phone ringtone, which briefly plays at specific times during the 10-minute alerting period. The alerting ringtone plays at the user-designated volume level. The audible alert schedule is:  
  - 10 minutes before power down, play the ringtone four times.  
  - 7 minutes before power down, play the ringtone four times.  
  - 4 minutes before power down, play the ringtone four times.  
  - 30 seconds before power down, play the ringtone 15 times or until the phone powers down.  
This check box applies only if the Enable Power Save Plus list box has one or more days selected. |
<p>| EnergyWise Domain | The EnergyWise domain that the phone is in. The maximum length is 127 characters.                                                        |
| EnergyWise Secret | The security secret password that is used to communicate with the endpoints in the EnergyWise domain. The maximum length is 127 characters. |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow EnergyWise Overrides</td>
<td>This check box determines if you will allow the EnergyWise domain controller policy to send power level updates to the phones. The following conditions apply:</td>
</tr>
<tr>
<td></td>
<td>1 If the phone is in full power save mode and the level is set to any standby level, the phone will go to Power Save when idle and remain in that mode until the next Cisco Unified CM scheduled power level change or user interaction.</td>
</tr>
<tr>
<td></td>
<td>2 If the phone is in Power Save or at full power and the level is set to any nonoperational level, the phone will power down when idle and remain powered off until the switch reapplies power or the user wakes the phone.</td>
</tr>
</tbody>
</table>

For example, assume the Phone Off Time is set to 22:00 (10:00 p.m.), the value in the Phone On Time field is 06:00 (6:00 a.m.), and the Enable Power Save Plus has one or more days selected.

- If EnergyWise directs the phone to turn off at 20:00 (8:00 p.m.), then the directive remains in effect until the configured Phone On Time at 6:00 a.m., assuming no phone user intervention occurs.
- At 6 a.m., the phone will turn on and resume receiving its power level changes from the settings in Cisco Unified Communications Manager Administration.
- To change the power level on the phone again, EnergyWise must reissue a new power level change command.

**Note** To disable Power Save Plus, you must uncheck the Allow EnergyWise Overrides check box. Leaving the Allow EnergyWise Overrides checked with no days selected in the Enable Power Save Plus field does not disable Power Save Plus.

---

**UCR 2008 Setup**

You configure the parameters that support UCR 2008 in Cisco Unified Communications Manager Administration. The following table describes the parameters and indicates the procedure to change the setting.
### Table 40: UCR 2008 Parameter Location

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Administration path</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIPS Mode</td>
<td>Device &gt; Device Settings &gt; Common Phone Profile</td>
<td>Set Up UCR 2008 in Common Phone Profile Configuration Window, on page 164</td>
</tr>
<tr>
<td></td>
<td>System &gt; Enterprise Phone Configuration</td>
<td>Set Up UCR 2008 in Enterprise Phone Configuration Window, on page 164</td>
</tr>
<tr>
<td>SSH Access</td>
<td>Device &gt; Phone</td>
<td>Set Up UCR 2008 in Phone Configuration Window, on page 163</td>
</tr>
<tr>
<td></td>
<td>Device &gt; Device Settings &gt; Common Phone Profile</td>
<td>Set Up UCR 2008 in Common Phone Profile Configuration Window, on page 164</td>
</tr>
<tr>
<td>Web Access</td>
<td>Device &gt; Phone</td>
<td>Set Up UCR 2008 in Phone Configuration Window, on page 163 Control Web Page Access, on page 201</td>
</tr>
<tr>
<td>HTTPS Server</td>
<td>Device &gt; Phone</td>
<td>Set Up UCR 2008 in Phone Configuration Window, on page 163</td>
</tr>
<tr>
<td></td>
<td>System &gt; Enterprise Phone Configuration</td>
<td>Set Up UCR 2008 in Enterprise Phone Configuration Window, on page 164</td>
</tr>
<tr>
<td>80-bit SRTCP</td>
<td>Device &gt; Device Settings &gt; Common Phone Profile</td>
<td>Set Up UCR 2008 in Common Phone Profile Configuration Window, on page 164</td>
</tr>
<tr>
<td></td>
<td>System &gt; Enterprise Phone Configuration</td>
<td>Set Up UCR 2008 in Enterprise Phone Configuration Window, on page 164</td>
</tr>
<tr>
<td>IP Addressing Mode</td>
<td>Device &gt; Device Settings &gt; Common Device Configuration</td>
<td>See Network Configuration Menu, on page 66.</td>
</tr>
<tr>
<td>IP Addressing Mode Preference for Signaling</td>
<td>Device &gt; Device Settings &gt; Common Device Configuration</td>
<td>See Network Configuration Menu, on page 66.</td>
</tr>
</tbody>
</table>

## Set Up UCR 2008 in Phone Configuration Window

Use this procedure to set the following parameters:

- SSH Access
- Web Access
- HTTPS Server
Set Up UCR 2008 in Common Phone Profile Configuration Window

Use this procedure to set the following parameters:

- FIPS Mode
- SSH Access
- 80-bit SRTCP

**Procedure**

**Step 1** Choose Device > Phone.
**Step 2** Set the SSH Access parameter to Disabled.
**Step 3** Set the Web Access parameter to Disabled.
**Step 4** Set the HTTPS Service parameter to HTTPS only.
**Step 5** Click Save.

Set Up UCR 2008 in Enterprise Phone Configuration Window

Use this procedure to set the following parameters:

- FIPS Mode
- HTTPS Server
- 80-bit SRTCP

**Procedure**

**Step 1** Choose Device > Device Settings > Common Phone Profile.
**Step 2** Set the FIPS Mode parameter to Enabled.
**Step 3** Set the SSH Access parameter to Disabled.
**Step 4** Set the 80-bit SRTCP parameter to Enabled.
**Step 5** Click Save.
## Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose <strong>System &gt; Enterprise Phone Configuration</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Set the FIPS Mode parameter to <strong>Enabled</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Set the HTTPS Server parameters to <strong>HTTPS only</strong>.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Set the 80-bit SRTCP parameter to <strong>Enabled</strong>.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click <strong>Save</strong>.</td>
</tr>
</tbody>
</table>
Set Up UCR 2008 in Enterprise Phone Configuration Window
CHAPTER 6

Cisco Unified IP Phone Customization

- Configuration File Customization and Modification, page 167
- Custom Phone Ring Creation, page 168
- Custom Background Images, page 170
- Wideband Codec Setup, page 172
- Idle Display Setup, page 173
- Cisco Unified IP Phone Backlight, page 174

Configuration File Customization and Modification

You can modify configuration files and add customized files to the TFTP directory. You can modify files or add customized files to the TFTP directory in Cisco Unified Communications Operating System Administration, from the TFTP Server File Upload window. For information about how to upload files to the TFTP folder on a Cisco Unified Communications Manager server, see the Cisco Unified Communications Manager System Guide.

You can obtain a copy of the Ringlist.xml or Ringlist-wb.xml files and the List.xml file from the system using the following admin command-line interface (CLI) “file” commands:

- admin:file
  * file list
  * file view
  * file search
  * file get
  * file dump
  * file tail
  * file delete

For more information, see the Cisco Intercompany Media Engine Command Line Interface Reference Guide.
Custom Phone Ring Creation

The Cisco Unified IP Phone ships with two default ring types that are implemented in hardware: Chirp1 and Chirp2. Cisco Unified Communications Manager also provides a default set of additional phone ring sounds that are implemented in software as pulse code modulation (PCM) files. The PCM files, along with an XML file (named Ringlist.xml) that describes the ring list options that are available at your site, exist in the TFTP server on each Cisco Unified Communications Manager server.

For more information, see the “Custom Phone Rings” chapter in the *Cisco Unified Communications Manager Features and Services Guide* and the “Software Upgrades” chapter in the *Cisco Unified Communications Operating System Administration Guide*.

The following sections describe how you can customize the phone rings that are available at your site by creating PCM files and editing the Ringlist.xml file:

Ringlist.xml File Format Requirements

The Ringlist.xml file defines an XML object that contains a list of phone ring types. This file includes up to 50 ring types. Each ring type contains a pointer to the PCM file that is used for that ring type and the text that appears on the Ring Type menu on a Cisco Unified IP Phone for that ring. The Cisco TFTP server for each Cisco Unified Communications Manager contains this file.

The CiscoIPPhoneRinglist XML object uses the following simple tag set to describe the information:

```xml
<CiscoIPPhoneRingList>
<Ring>
  <DisplayName/>
  <FileName/>
</Ring>
</CiscoIPPhoneRingList>
```

The following characteristics apply to the definition names. You must include the required DisplayName and FileName for each phone ring type.

- **DisplayName** specifies the name of the custom ring for the associated PCM file that displays on the Ring Type menu of the Cisco Unified IP Phone.
- **FileName** specifies the name of the PCM file for the custom ring to associate with DisplayName.

Note

The DisplayName and FileName fields must not exceed 25 characters in length.

This example shows a Ringlist.xml file that defines two phone ring types:

```xml
<CiscoIPPhoneRingList>
  <Ring>
    <DisplayName>Analog Synth 1</DisplayName>
    <FileName>Analog1.raw</FileName>
  </Ring>
  <Ring>
    <DisplayName>Analog Synth 2</DisplayName>
    <FileName>Analog2.raw</FileName>
  </Ring>
</CiscoIPPhoneRingList>
```
PCM File Requirements for Custom Ring Types

The PCM files for the rings must meet the following requirements for proper playback on Cisco Unified IP Phones:

- Raw PCM (no header)
- 8000 samples per second
- 8 bits per sample
- Mu-law compression
- Maximum ring size = 16080 samples
- Minimum ring size = 240 samples
- Number of samples in the ring = multiple of 240.
- Ring start and end at zero crossing.

To create PCM files for custom phone rings, use any standard audio editing package that supports these file format requirements.

Set Up Custom Phone Ring

To create custom phone rings for the Cisco Unified IP Phone, perform these steps:

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Create a PCM file for each custom ring (one ring per file). Ensure the PCM files comply with the format guidelines that are listed in PCM File Requirements for Custom Ring Types, on page 169.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Upload the new PCM files that you created to the Cisco TFTP server for each Cisco Unified Communications Manager in your cluster. For more information, see the “Software Upgrades” chapter in Cisco Unified Communications Operating System Administration Guide.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Use a text editor to edit the Ringlist.xml file. See Ringlist.xml File Format Requirements, on page 168 for information about how to format this file and for a sample Ringlist.xml file.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Save your modifications and close the Ringlist.xml file.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>To cache the new Ringlist.xml file, stop and start the TFTP service by using Cisco Unified Serviceability or disable and reenable the “Enable Caching of Constant and Bin Files at Startup” TFTP service parameter (that is found in the Advanced Service Parameters area.)</td>
</tr>
</tbody>
</table>
Custom Background Images

You can provide users with a choice of background images for the LCD screen on their phones. Users can select a background image by choosing Settings > User Preferences > Background Images on the phone.

The image choices that users see come from PNG images and an XML file (called List.xml) that are stored on the TFTP server that the phone uses. By storing your own PNG files and editing the XML file on the TFTP server, you can designate the background images from which users can choose. In this way, you can provide custom images, such as your company logo.

The following sections describe how you can customize the background images that are available at your site by creating your own PNG files and editing the List.xml file.

List.xml File Format Requirements

The List.xml file defines an XML object that contains a list of background images. The List.xml file is stored in the following subdirectory on the TFTP server:

- /Desktops/320x212x16 for Cisco Unified IP Phone 7945 and 7965
- /Desktops/320x212x12 for Cisco Unified IP Phone 7971 and 7970
- /Desktops/320x212x12 for Cisco Unified IP Phone 7975

Tip

If you are manually creating the directory structure and the List.xml file, you must ensure that the directories and files can be accessed by the user CCMService, which is used by the TFTP service.

For more information, see "Software Upgrades" chapter in Cisco Unified Communications Operating System Administration Guide.

The List.xml file can include up to 50 background images. The images are in the order that they appear in the Background Images menu on the phone. For each image, the List.xml file contains one element type, called ImageItem. The ImageItem element includes these two attributes:

- Image: Uniform resource identifier (URI) that specifies where the phone obtains the thumbnail image that will appear on the Background Images menu on a Phone.
- URL: URI that specifies where the phone obtains the full-size image.

The following example (for a Cisco Unified IP Phone 7971G-GE and 7970G) shows a List.xml file that defines two images. The required Image and URL attributes must be included for each image. The TFTP URI that displays in the example is the only supported method for linking to full size and thumbnail images. HTTP URL support is not provided.

List.xml Example

```xml
<CiscoIPPhoneImageList>
    <ImageItem Image="TFTP:Desktops/320x212x12/TN-Fountain.png" URL="TFTP:Desktops/320x212x12/Fountain.png"/>
    <ImageItem Image="TFTP:Desktops/320x212x12/TN-FullMoon.png" URL="TFTP:Desktops/320x212x12/FullMoon.png"/>
</CiscoIPPhoneImageList>
```
The Cisco Unified IP Phone firmware includes a default background image. This image is not defined in the List.xml file. The default image is always the first image that appears in the Background Images menu on the phone.

**PNG File Requirements for Custom Background Images**

Each background image requires two PNG files:

- **Full size image**: Version that displays on the on the phone.
- **Thumbnail image**: Version that displays on the Background Images screen from which users can select an image. The thumbnail image must be 25% of the size of the full-size image.

**Tip**

Many graphics programs provide a feature that will resize a graphic. An easy way to create a thumbnail image is to first create and save the full size image, then use the sizing feature in the graphics program to create a version of that image that is 25% of the original size. Save the thumbnail version with a different name than the full-size image.

The PNG files for background images must meet the following requirements for proper display on the Cisco Unified IP Phone:

- **Full size image**: 320 pixels (width) X 216 pixels (height)
- **Thumbnail image**: 80 pixels (width) X 53 pixels (height)
- **Color palette**:
  - For Cisco Unified IP Phone 7971G-GE and 7970G)—Includes up to 12-bit color (4096 colors). You can use more than 12-bit color, but the phone will reduce the color palette to 12-bit before displaying the image. For best results, reduce the color palette of an image to 12-bit when you create a PNG file.
  
  **Tip**: If you are using a graphics program that supports a posterize feature for specifying the number of tonal levels per color channel, set the number of tonal levels per channel to 16 (16 red X 16 green X 16 blue = 4096 colors).

  - For Cisco Unified IP Phone 7975G, 7965G, and 7945G)—Includes up to 16-bit color (65535 colors). You can use more than 16-bit color, but the phone will reduce the color palette to 16-bit before displaying the image. For best results, reduce the color palette of an image to 16-bit when you create a PNG file.

  **Tip**: If you are using a graphics program that supports a posterize feature for specifying the number of tonal levels per color channel, set the number of tonal levels per channel to 40 (40 red X 40 green X 40 blue = 64000 colors). This is as close as you can posterize to 65535 colors without exceeding the maximum.

**Set Up Custom Background Image**

To create custom background images for the Cisco Unified IP Phone, follow these steps:
Procedure

Step 1 Create two PNG files for each image (a full size version and a thumbnail version). Ensure the PNG files comply with the format guidelines that are listed in PNG File Requirements for Custom Background Images, on page 171.

Step 2 Upload the new PNG files that you created to the following subdirectory in the TFTP server for Cisco Unified Communications Manager:

- /Desktops/320x216x16 for Cisco Unified IP Phone 7975G
- /Desktops/320x212x16 for Cisco Unified IP Phone 7965G and 7945G

Note The file name and subdirectory parameters are case sensitive. Be sure to use the forward slash "/" when you specify the subdirectory path.

To upload the files, choose Software Upgrades > Upload TFTP Server File in Cisco Unified Communications Operating System Administration. For more information, see the "Software Upgrade" chapter in Cisco Unified Communications Operating System Administration Guide.

Step 3 You must also copy the customized images and files to the other TFTP servers that the phone may contact to obtain these files.

Note Cisco recommends that you also store backup copies of custom image files in another location. You can use these backup copies if the customized files are overwritten when you upgrade Cisco Unified Communications Manager.

Step 4 Use a text editor to edit the List.xml file. See List.xml File Format Requirements, on page 170 for the location of this file, formatting requirements, and a sample file.

Step 5 Save your modifications and close the List.xml file.

Note When you upgrade Cisco Unified Communications Manager, a default List.xml file will replace your customized List.xml file. After you customize the List.xml file, make a copy of the file and store it in another location. After upgrading Cisco Unified Communications Manager, replace the default List.xml file with your stored copy.

Step 6 To cache the new List.xml file, stop and start the TFTP service by using Cisco Unified Serviceability or disable and re-enable the Enable Caching of Constant and Bin Files at Startup TFTP service parameter (located in the Advanced Service Parameters).

Wideband Codec Setup

If Cisco Unified Communications Manager has been configured to use G.722 (G.722 is enabled by default for the Cisco Unified IP Phone) and if the far endpoint supports G.722, the call can connect using the G.722 codec in place of G.711. This situation occurs regardless of whether the user has enabled a wideband headset or wideband handset, but if either the headset or handset is enabled, the user may notice greater audio sensitivity during the call. Greater sensitivity means improved audio clarity but also means that more background noise can be heard by the far endpoint: noise such as rustling papers or nearby conversations. Even without a wideband headset or handset, some users may prefer the additional sensitivity of G.722. Other users may be distracted by the additional sensitivity of G.722.
Two parameters in Cisco Unified Communications Manager Administration affect whether wideband is supported for this Cisco Unified Communications Manager server or a specific phone:

- **Advertise G.722 Codec**: From Cisco Unified Communications Manager Administration, choose **System > Enterprise Parameters**. The default value of this enterprise parameter is True, which means that all Cisco Unified IP Phone models that are described in this administration guide and are registered to this Cisco Unified Communications Manager will advertise G.722 to Cisco Unified Communications Manager. For more information, see the *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones" chapter.

- **Advertise G.722 Codec**: From Cisco Unified Communications Manager Administration, choose **Device > Phone**. The default value of this product-specific parameter is to use the value specified in the enterprise parameter. If you want to override this on a per-phone basis, choose Enabled or Disabled in the advertises G.722 Codec parameter on the Product Specific Configuration area of the Phone Configuration window.

## Idle Display Setup

You can specify an idle display that appears on the phone LCD screen. The idle display is an XML service that the phone invokes when the phone has been idle (not in use) for a designated period and no feature menu is open.

XML services that can be used as idle displays include company logos, product pictures, and stock quotes.

Configuration of the idle display requires these general steps:

1. Format an image for display on the phone.
2. Configure Cisco Unified Communications Manager to display the image on the phone.

For detailed instructions about creating and displaying the idle display, see *Creating Idle URL Graphics on Cisco Unified IP Phone* at this URL:


In addition, see the *Cisco Unified Communications Manager Administration Guide* or the *Cisco Unified Communications Manager Bulk Administration Guide* for the following information:

- Specify the URL of the idle display XML service:
  - For a single phone: Idle field in the Cisco Unified Communications Manager Phone Configuration window
  - For multiple phones simultaneously: URL Idle field on the Cisco Unified Communications Manager Enterprise Parameters configuration window, or the Idle field in the Bulk Administration Tool (BAT)

- Specify the length of time that the phone is not used before the idle display XML service is invoked:
  - For a single phone: Idle Timer field on the Cisco Unified Communications Manager Phone configuration window
  - For multiple phones simultaneously: URL Idle Time field on the Cisco Unified Communications Manager Enterprise Parameters configuration window, or the Idle Timer field in the Bulk Administration Tool (BAT)
From a phone, you can see settings for the idle display XML service URL and the length of time that the phone is not used before this service is invoked. To see these settings, choose Settings > Device Configuration and scroll to the Idle URL and the Idle URL Time parameters.

## Cisco Unified IP Phone Backlight

To conserve power and ensure the longevity of the LCD screen on the phone, you can set the LCD to turn off when it is not needed.

You can configure settings in Cisco Unified Communications Manager Administration to turn off the display at a designated time on some days and all day on other days. For example, you may choose to turn off the display after business hours on weekdays and all day on Saturdays and Sundays.

When the display is off, the LCD screen is dark and disabled, and the Display button lights. You can take any of these actions to turn on the display any time it is off:

- Press any button on the phone.
  - If you press a button other than the Display button, the phone will take the action designated by that button in addition to turning on the display.
- Touch the touchscreen (or phone screen, whichever is applicable).
- Lift the handset.

When you turn the display on, it remains on until the phone remains idle for a designated length of time, then it turns off automatically.

---

**Note**

You can use the Display button to temporarily disable the touchscreen (or phone screen) for cleaning. See Cisco Unified IP Phone Cleaning, on page 241 for more information.

---

**Note**

The XSI Screen Width Enhancement feature, when implemented on Cisco Unified IP Phones, enhances the viewability of the Messages, Directories, and Services screens. These screens may appear in Normal mode or in Wide mode, depending on how the phone is set up. For information, see the Cisco Unified IP Phone Services Application Development Notes at http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_programming_reference_guides_list.html.

The following table explains the Cisco Unified Communications Manager Administration fields that control when the display turns on and off. You configure these fields in Cisco Unified Communications Manager Administration in the Product Specific configuration window. (You access this window by choosing Device > Phone from Cisco Unified Communications Manager Administration.)

You can view the display settings for a phone from the Power Save Configuration menu on the phone. For more information, see Power Save Configuration Menu, on page 99.
### Table 41: Display On and Off configuration fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Days Display Not Active</td>
<td>Days that the display does not turn on automatically at the time specified in the Display On Time field. Choose the day or days from the drop-down list. To choose more than one day, Ctrl-click each day that you want.</td>
</tr>
<tr>
<td>Display On Time</td>
<td>Time each day that the display turns on automatically (except on the days specified in the Days Display Not Active field). Enter the time in this field in 24 hour format, where 0:00 is midnight. For example, to automatically turn the display on at 7:00 a.m., enter 7:00. To turn the display on at 2:00 p.m., enter 14:00. If this field is blank, the display will automatically turn on at 0:00.</td>
</tr>
<tr>
<td>Display On Duration</td>
<td>Length of time that the display remains on after turning on at the time specified in the Display On Time field. Enter the value in this field in the format hours:minutes. For example, to keep the display on for 4 hours and 30 minutes after it turns on automatically, enter 4:30. If this field is blank, the phone will turn off at the end of the day (0:00). <strong>Note</strong> If Display On Time is 0:00 and the display on duration is blank (or 24:00), the display stays on continuously.</td>
</tr>
<tr>
<td>Display Idle Timeout</td>
<td>Length of time that the phone is idle before the display turns off. Applies only when the display was off as scheduled and was turned on by an end user by pressing a button on the phone, touching the touchscreen or phone screen, or lifting the handset. Enter the value in this field in the format hours:minutes. For example, to turn the display off when the phone is idle for 1 hour and 30 minutes after an end user turns the display on, enter 1:30. The default value is 0:30.</td>
</tr>
<tr>
<td>Display On When Incoming Call</td>
<td>Disable/enable automatic illumination of the LCD screen when a call is received. Default: Disabled</td>
</tr>
</tbody>
</table>
Model Information, Status, and Statistics

- Model Information, Status, and Statistics Overview, page 177
- Display Model Information Screen, page 178
- Status Menu, page 179
- Test Tone, page 196

Model Information, Status, and Statistics Overview

This chapter describes how to use the following menus and screens on the Cisco Unified IP Phone to view model information, status messages, network statistics, and firmware information for the phone:

- Model Information screen: Displays hardware and software information about the phone.
- Status menu: Provides access to screens that display the status messages, network statistics, and firmware versions.
- Call Statistics screen: Displays counters and statistics for the current call.

You can use the information 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. For more information, see Remote Monitoring, on page 199.

For more information about troubleshooting the Cisco Unified IP Phone, see Troubleshooting and Maintenance, on page 217.
Display Model Information Screen

Procedure

Step 1  To display the Model Information screen, press the **Settings** button and then select **Model Information**.

Step 2  To exit the Model Information screen, press **Exit**.

Model Information Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model Number</td>
<td>Model number of the phone.</td>
<td>Display only. Cannot configure.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>MAC address of the phone.</td>
<td>Display only. Cannot configure.</td>
</tr>
<tr>
<td>Load File</td>
<td>Identifier of the factory-installed load running on the phone.</td>
<td>Display only. Cannot configure.</td>
</tr>
<tr>
<td>Boot Load ID</td>
<td>Identifier of the factory-installed load running on the phone.</td>
<td>Display only. Cannot configure.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Serial number of the phone.</td>
<td>Display only. Cannot configure.</td>
</tr>
<tr>
<td>MIC</td>
<td>Indicates whether a manufacturing installed certificate is present on the phone.</td>
<td>For more information about how to manage the MIC for your phone, see the &quot;Using the Certificate Authority Proxy Function&quot; chapter in Cisco Unified Communications Manager Security Guide.</td>
</tr>
<tr>
<td>LSC</td>
<td>Indicates whether a locally significant certificate is present on the phone.</td>
<td>For more information about how to manage the LSC for your phone, see the &quot;Using the Certificate Authority Proxy Function&quot; chapter in Cisco Unified Communications Manager Security Guide.</td>
</tr>
<tr>
<td>Call Control Protocol</td>
<td>Indicates the call processing protocol used by the phone.</td>
<td>For more information, see Cisco Unified IP Phones and Different Protocols, on page 40.</td>
</tr>
</tbody>
</table>
Status Menu

The Status menu includes these options, which provide information about the phone and its operation:

- Status Messages: Displays the Status Messages screen, which shows a log of important system messages.
- Network Statistics: Displays the Network Statistics screen, which shows Ethernet traffic statistics.
- Firmware Versions: Displays the Firmware Versions screen, which shows information about the firmware that is running on the phone.
- Expansion Modules: Displays the Expansion Modules screen, which shows information about the Cisco Unified IP Phone Expansion Modules, if connected to the phone.

Related Topics

Status Messages Screen, on page 179
Network Statistics Screen, on page 188
Expansion Modules Screen, on page 192
Firmware Version Screen, on page 191

Display Status Menu

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Press Apps.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Select Admin Settings &gt; Status Menu.</td>
</tr>
</tbody>
</table>

Status Messages Screen

The Status Messages screen displays the 10 most recent status messages that the phone has generated. You can access this screen at any time, even if the phone has not finished starting up. See Status Messages, on page 180, which describes the status messages that might display. This table also includes actions that you can take to address errors.

Display Status Messages Screen

To display the Status Messages screen, follow these steps:
Procedure

**Step 1** Press **Settings**.
**Step 2** Select **Status**.
**Step 3** Select **Status Messages**.
**Step 4** To remove current status messages, press **Clear**.
**Step 5** To exit the Status Messages screen, press **Exit**.

Status Messages

Table 43: Status Messages on the Cisco Unified IP Phone

<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
<th>Possible explanation and action</th>
</tr>
</thead>
<tbody>
<tr>
<td>BootP server used</td>
<td>The phone obtained its IP address from a BootP server rather than a DHCP server.</td>
<td>None. This message is informational only.</td>
</tr>
<tr>
<td>CFG file not found</td>
<td>The name-based and default configuration file was not found on the TFTP Server.</td>
<td>Cisco Unified Communications Manager creates a configuration file for the phone with the phone is added to the database. If the phone has not been added to the Cisco Unified Communications Manager database, the TFTP server generates a CFG File Not Found response.</td>
</tr>
</tbody>
</table>

- Phone is not registered with Cisco Unified Communications Manager. You must manually add the phone to Cisco Unified Communications Manager if you are not allowing phones to autoregister. See Cisco Unified Communications Manager Administration Phone Addition, on page 39 for details.
- If you are using DHCP, verify that the DHCP server is pointing to the correct TFTP server.
- If you are using static IP addresses, check configuration of the TFTP server. See Network Configuration Menu, on page 66 for details on assigning a TFTP server.
<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
<th>Possible explanation and action</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFG TFTP Size Error</td>
<td>The configuration file is too large for the file system on the phone.</td>
<td>Power cycle the phone.</td>
</tr>
<tr>
<td>Checksum Error</td>
<td>Downloaded software file is corrupted.</td>
<td>Obtain a new copy of the phone firmware and place it in the TFTP directory. You should only copy files into this directory when the TFTP server software is shut down, otherwise the files may be corrupted.</td>
</tr>
<tr>
<td>CTL and ITL installed</td>
<td>CTL and ITL files are installed on the phone.</td>
<td>None. This message is informational only. Neither the CTL file nor the ITL file was installed on the phone previously. For more information about the Trust List, see the Cisco Unified Communications Manager Security Guide.</td>
</tr>
<tr>
<td>CTL installed</td>
<td>The CTL file is installed on the phone.</td>
<td>None. This message is informational only. The CTL file was not installed previously. For more information about the CTL file, see the Cisco Unified Communications Manager Security Guide.</td>
</tr>
</tbody>
</table>
| DHCP timeout     | DHCP server did not respond.                         | • Network is busy: The errors should resolve themselves when the network load reduces.  
• No network connectivity between the DHCP server and the phone: Verify the network connections.  
• DHCP server is down: Check configuration of DHCP server.  
• Errors persist: Consider assigning a static IP address. See Network Configuration Menu, on page 66 for details on assigning a static IP address. |
<p>| Disabled         | 802.1X Authentication is disabled on the phone.       | You can enable 802.1X authentication by using the Settings &gt; Security Configuration &gt; 802.1X Authentication option on the phone. For more information, see 802.1X Authentication and Status Menus, on page 116. |</p>
<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
<th>Possible explanation and action</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS timeout</td>
<td>DNS server did not respond.</td>
<td>Network is busy: The errors should resolve themselves when the network load reduces. No network connectivity between the DNS server and the phone: Verify the network connections. DNS server is down: Check configuration of DNS server.</td>
</tr>
<tr>
<td>DNS unknown host</td>
<td>DNS could not resolve the name of the TFTP server or Cisco Unified Communications Manager.</td>
<td>Verify that the host names of the TFTP server or Cisco Unified Communications Manager are configured properly in DNS. Consider using IP addresses rather than host names.</td>
</tr>
<tr>
<td>Duplicate IP</td>
<td>Another device is using the IP address assigned to the phone.</td>
<td>If the phone has a static IP address, verify that you have not assigned a duplicate IP address. See Network Configuration Menu, on page 66 for details. If you are using DHCP, check the DHCP server configuration.</td>
</tr>
<tr>
<td>Erasing CTL and ITL files</td>
<td>Erasing CTL or ITL file.</td>
<td>None. This message is informational only. For more information about the CTL and ITL files, see the Cisco Unified Communications Manager Security Guide.</td>
</tr>
</tbody>
</table>
| Error update locale     | One or more localization files could not be found in the TFTP directory or were not valid. The locale was not changed. | From Cisco Unified Operating System Administration, check that the following files are located within the subdirectories in TFTP File Management:  
  • Located in subdirectory with same name as network locale:  
    • tones.xml  
  • Located in subdirectory with same name as user locale:  
    • glyphs.xml  
    • dictionary.xml  
    • kate.xml |
<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
<th>Possible explanation and action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failed</td>
<td>The phone attempted an 802.1X transaction but authentication failed.</td>
<td>Authentication typically fails for one of the following reasons:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• No shared secret is configured in the phone or authentication server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The shared secret configured in the phone and the authentication server do not match.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Phone has not been configured in the authentication server.</td>
</tr>
<tr>
<td>File auth error</td>
<td>An error occurred when the phone tried to validate the signature of a signed file. This message includes the name of the file that failed.</td>
<td>The file is corrupted. If the file is a phone configuration file, delete the phone from the Cisco Unified Communications Manager database by using Cisco Unified Communications Manager Administration. Then add the phone back to the Cisco Unified Communications Manager database by using Cisco Unified Communications Manager Administration. The CTL file has a problem and the key for the server from which files are obtained is bad. In this case, run the CTL client and update the CTL file, making sure that the proper TFTP servers are included in this file.</td>
</tr>
<tr>
<td>File not found</td>
<td>The phone cannot locate, on the TFTP server, the phone load file that in the phone configuration file specifies.</td>
<td>From Cisco Unified Operating System Administration, ensure that the TFTP File Management lists the phone load file.</td>
</tr>
<tr>
<td>IP address released</td>
<td>The phone has been configured to release its IP address.</td>
<td>The phone remains idle until it is power cycled or you reset the DHCP address. See Network Configuration Menu, on page 66 for details.</td>
</tr>
<tr>
<td>ITL installed</td>
<td>The ITL file is installed in the phone. The ITL file was not installed.</td>
<td>None. This message is informational only. Phone does not have prior installation of the ITL file.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For more information about the ITL file, see the Cisco Unified Communications Manager Security Guide.</td>
</tr>
</tbody>
</table>
### Possible explanation and action

**ITL update failed**  
Updating ITL file failed.  
Phone has CTL or ITL file installed and it failed to update new ITL file.  
**Possible reasons for failure:**  
- Network failure  
- TFTP server was down  
- Trust Verification Service (TVS) server was down  
**Possible solutions:**  
- Check the network connectivity.  
- Check whether the TFTP server is active and functioning normally.  
- Check whether the Trust Verification Service (TVS) server is active and functioning normally.  
- Manually delete CTL and ITL files if all the above solutions fail.

**Load Auth Failed**  
The phone could not load a configuration file.  
Check that:  
- A good version of the configuration file exists on the applicable server.  
- The phone load being downloaded has not been altered or renamed.  
- Phone load type is compatible; for example, you cannot place a DEV load configuration file on a REL-signed phone.

**Load ID incorrect**  
Load ID of the software file is of the wrong type.  
Check the load ID assigned to the phone (from Cisco Unified Communications Manager, choose **Device > Phone**). Verify that the load ID is entered correctly.
<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
<th>Possible explanation and action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Load rejected HC</td>
<td>The application that was downloaded is not compatible with the phone hardware.</td>
<td>Occurs if you were attempting to install a version of software on this phone that did not support hardware changes on this newer phone. Check the load ID assigned to the phone (from Cisco Unified Communications Manager, choose <strong>Device &gt; Phone</strong>). Re-enter the load displayed on the phone. See <strong>Firmware Version Screen</strong>, on page 191 to verify the phone setting.</td>
</tr>
<tr>
<td>Load Server is invalid</td>
<td>Indicates an invalid TFTP server IP address or name in the Load Server option.</td>
<td>The Load Server setting is not valid. The Load Server specifies a TFTP server IP address or name from which the phone firmware can be retrieved for upgrades on the phones. Check the Load Server entry (from Cisco Unified Communications Manager Administration choose <strong>Device &gt; Phone</strong>).</td>
</tr>
<tr>
<td>No default router</td>
<td>DHCP or static configuration did not specify a default router.</td>
<td>If the phone has a static IP address, verify that the default router has been configured. See <strong>Network Configuration Menu</strong>, on page 66 for details. If you are using DHCP, the DHCP server has not provided a default router. Check the DHCP server configuration.</td>
</tr>
<tr>
<td>No DNS server IP</td>
<td>A name was specified but DHCP or static IP configuration did not specify a DNS server address.</td>
<td>If the phone has a static IP address, verify that the DNS server has been configured. See <strong>Network Configuration Menu</strong>, on page 66 for details. If you are using DHCP, the DHCP server has not provided a DNS server. Check the DHCP server configuration.</td>
</tr>
<tr>
<td>No Trust List installed</td>
<td>The Trust List is not configured on Cisco Unified Communications Manager, which does not support security by default.</td>
<td>Occurs if the Trust List is not configured on Cisco Unified Communications Manager and Cisco Unified Communications Manager does not support security by default. For more information about CTL and ITL files, see the <strong>Cisco Unified Communications Manager Security Guide</strong>.</td>
</tr>
<tr>
<td>Message</td>
<td>Description</td>
<td>Possible explanation and action</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Programming Error</td>
<td>The phone failed during programming.</td>
<td>Attempt to resolve this error by power cycling the phone. If the problem persists, contact Cisco technical support for additional assistance.</td>
</tr>
<tr>
<td>Successful – MD5</td>
<td>The phone attempted an 802.1X transaction and authentication achieved.</td>
<td>The phone achieved 802.1X authentication.</td>
</tr>
<tr>
<td>TFTP access error</td>
<td>TFTP server is pointing to a directory that does not exist.</td>
<td>If you are using DHCP, verify that the DHCP server points to the correct TFTP server. If you are using static IP addresses, check configuration of TFTP server. See Network Configuration Menu, on page 66 for details on assigning a TFTP server.</td>
</tr>
<tr>
<td>TFTP Error</td>
<td>The phone does not recognize an error code provided by the TFTP server.</td>
<td>Contact the Cisco TAC.</td>
</tr>
<tr>
<td>TFTP file not found</td>
<td>The requested load file (.bin) was not found in the TFTP directory.</td>
<td>Check the load ID assigned to the phone (from Cisco Unified Communications Manager, choose Device &gt; Phone). Verify that the TFTP directory contains a .bin file with this load ID as the name.</td>
</tr>
<tr>
<td>TFTP timeout</td>
<td>TFTP server did not respond.</td>
<td>Network is busy: The errors should resolve themselves when the network load reduces. No network connectivity between the TFTP server and the phone: Verify the network connections. TFTP server is down: Check configuration of TFTP server.</td>
</tr>
<tr>
<td>Timed Out</td>
<td>Supplicant attempted 802.1X transaction but timed out due the absence of an authenticator.</td>
<td>Authentication typically times out if 802.1X authentication is not configured on the switch.</td>
</tr>
<tr>
<td>Message</td>
<td>Description</td>
<td>Possible explanation and action</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Trust List update failed</td>
<td>The CTL and ITL files are installed on the phone, and it failed to update</td>
<td>Phone has CTL and ITL files installed and it failed to update the new CTL and ITL files.</td>
</tr>
<tr>
<td></td>
<td>the new files.</td>
<td><strong>Possible reasons for failure:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Network failure.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• TFTP server was down.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The new security token used to sign CTL file and the TFTP certificate used to sign ITL file are introduced, but are not available in the current CTL and ITL files in the phone.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Internal phone failure.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Possible solutions:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Check the network connectivity.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Check if the TFTP server is active and functioning normally.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If the Trust Verification Service (TVS) server is supported on Cisco Unified Communications Manager, check if the TVS server is active and functioning normally.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Verify if the security token and the TFTP server are valid.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Manually delete the CTL and ITL files if all the above solutions fail, and reset the phone.</td>
</tr>
<tr>
<td>Trust List updated</td>
<td>The CTL file, the ITL file, or both files are updated.</td>
<td>None. This message is informational only.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For more information about the Trust List, see the Cisco Unified Communications Manager Security Guide.</td>
</tr>
<tr>
<td>Version error</td>
<td>The name of the phone load file is incorrect.</td>
<td>Make sure that the phone load file has the correct name.</td>
</tr>
<tr>
<td>XmlDefault corresponding to</td>
<td>Name of the configuration file.</td>
<td>None. This is an informational message indicating the name of the configuration file for the phone.</td>
</tr>
<tr>
<td>the phone device name</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

Network Statistics Screen

The Network Statistics screen displays information about the phone and network performance. Network Statistics Items, on page 188 describes the information that displays in this screen.

Display Network Statistics Screen

To display the Network Statistics screen, perform these steps:

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Press Applications.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select Settings.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select Status.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Select Network Statistics.</td>
</tr>
<tr>
<td>Step 5</td>
<td>To reset the Rx Frames, Tx Frames, and Rx Broadcasts statistics to 0, press Clear.</td>
</tr>
</tbody>
</table>

Network Statistics Items

The following table describes the Network Statistics items.

Table 44: Network Statistics Information

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rx Frames</td>
<td>Number of packets that the phone receives</td>
</tr>
<tr>
<td>Tx Frames</td>
<td>Number of packets that the phone sends</td>
</tr>
<tr>
<td>Rx Broadcasts</td>
<td>Number of broadcast packets that the phone receives</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>One of the following values:</td>
<td>Cause of the last phone reset</td>
</tr>
<tr>
<td>• Initialized</td>
<td></td>
</tr>
<tr>
<td>• TCP-timeout</td>
<td></td>
</tr>
<tr>
<td>• CM-closed-TCP</td>
<td></td>
</tr>
<tr>
<td>• TCP-Bad-ACK</td>
<td></td>
</tr>
<tr>
<td>• CM-reset-TCP</td>
<td></td>
</tr>
<tr>
<td>• CM-aborted-TCP</td>
<td></td>
</tr>
<tr>
<td>• CM-NAKed</td>
<td></td>
</tr>
<tr>
<td>• KeepaliveTO</td>
<td></td>
</tr>
<tr>
<td>• Failback</td>
<td></td>
</tr>
<tr>
<td>• Phone-Keypad</td>
<td></td>
</tr>
<tr>
<td>• Phone-Re-IP</td>
<td></td>
</tr>
<tr>
<td>• Reset-Reset</td>
<td></td>
</tr>
<tr>
<td>• Reset-Restart</td>
<td></td>
</tr>
<tr>
<td>• Phone-Reg-Rej</td>
<td></td>
</tr>
<tr>
<td>• Load Rejected HC</td>
<td></td>
</tr>
<tr>
<td>• CM-ICMP-Unreach</td>
<td></td>
</tr>
<tr>
<td>• Phone-Abort</td>
<td></td>
</tr>
<tr>
<td>Elapsed Time</td>
<td>Amount of time that has elapsed since the phone connected to Cisco Unified Communications Manager</td>
</tr>
<tr>
<td>Port 1</td>
<td>Link state and connection of the Network port</td>
</tr>
<tr>
<td>Port 2 (applies to 7911G only)</td>
<td>Link state and connection of the PC port. For example, Auto 100 Mb Full-Duplex means that the PC port is in a link up state and has autonegotiated a full-duplex, 100-Mbps connection.</td>
</tr>
</tbody>
</table>
IPv4

Information on the DHCP status. This includes the following states:

- CDP BOUND
- CDP INIT
- DHCP BOUND
- DHCP DISABLED
- DHCP INIT
- DHCP INVALID
- DHCP REBINDING
- DHCP REBOOT
- DHCP RENEWING
- DHCP REQUESTING
- DHCP RESYNC
- DHCP UNRECOGNIZED
- DHCP WAITING COLDBOOT TIMEOUT
- SET DHCP COLDBOOT
- SET DHCP DISABLED
- DISABLED DUPLICATE IP
- SET DHCP FAST
### IPv6

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6</td>
<td>Information on the DHCPv6 status. This includes the following states:</td>
</tr>
<tr>
<td></td>
<td>• DHCP6 BOUND;</td>
</tr>
<tr>
<td></td>
<td>• DHCP6 DISABLED</td>
</tr>
<tr>
<td></td>
<td>• DHCP6 RENEW</td>
</tr>
<tr>
<td></td>
<td>• DHCP6 REBIND</td>
</tr>
<tr>
<td></td>
<td>• DHCP6 INIT</td>
</tr>
<tr>
<td></td>
<td>• DHCP6 SOLICIT</td>
</tr>
<tr>
<td></td>
<td>• DHCP6 REQUEST</td>
</tr>
<tr>
<td></td>
<td>• DHCP6 RELEASING</td>
</tr>
<tr>
<td></td>
<td>• DHCP6 RELEASED</td>
</tr>
<tr>
<td></td>
<td>• DHCP6 DISABLING</td>
</tr>
<tr>
<td></td>
<td>• DHCP6 DECLINING</td>
</tr>
<tr>
<td></td>
<td>• DHCP6 DECLINED</td>
</tr>
<tr>
<td></td>
<td>• DHCP6 INFOREQ</td>
</tr>
<tr>
<td></td>
<td>• DHCP6 INFOREQ DONE</td>
</tr>
<tr>
<td></td>
<td>• DHCP6 INVALID</td>
</tr>
<tr>
<td></td>
<td>• DHCP6 DECLINED DUPLICATE IP</td>
</tr>
<tr>
<td></td>
<td>• DHCP6 WAITING COLDBOOT TIMEOUT</td>
</tr>
<tr>
<td></td>
<td>• DHCP6 TIMEOUT USING RESTORED VAL</td>
</tr>
<tr>
<td></td>
<td>• DHCP6 TIMEOUT. CANNOT RESTORE</td>
</tr>
<tr>
<td></td>
<td>• STACK TURNED OFF</td>
</tr>
</tbody>
</table>

---

**Firmware Version Screen**

The Firmware Version screen displays information about the firmware version that is running on the phone. [Firmware Version Items](#), on page 192 describes the information that displays on this screen.

**Display Firmware Version Screen**

To display the Firmware Version screen, follow these steps:
Procedure

**Step 1** Press **Settings**.

**Step 2** Select **Status**.

**Step 3** Select **Firmware Version**.

**Step 4** To exit the Firmware Version screen, press **Exit**.

Firmware Version Items

**Table 45: Firmware Version Information**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Load File</td>
<td>Load file running on the phone</td>
</tr>
<tr>
<td>App Load ID</td>
<td>JAR file running on the phone</td>
</tr>
<tr>
<td>JVM Load ID</td>
<td>Java Virtual Machine (JVM) running on the phone</td>
</tr>
<tr>
<td>OS Load ID</td>
<td>Operating system running on the phone</td>
</tr>
<tr>
<td>Boot Load ID</td>
<td>Factory-installed load running on the phone</td>
</tr>
<tr>
<td>Expansion Module 1</td>
<td>Load running on the Expansion Modules, if connected to a SIP or SCCP phone</td>
</tr>
<tr>
<td>Expansion Module 2</td>
<td>Load running on the Expansion Modules, if connected to a SIP or SCCP phone</td>
</tr>
<tr>
<td>DSP Load ID</td>
<td>Digital signal processor (DSP) software version used</td>
</tr>
</tbody>
</table>

Expansion Modules Screen

The Expansion Modules screen displays information about each Cisco Unified IP Phone Expansion Module that is connected to the phone.

Expansion Module Items, on page 193 explains the information displays on this screen for each connected expansion module. You can use this information to troubleshoot the expansion module, if necessary. In the Expansion Modules screen, a statistic preceded by "A" applies to the first expansion module. A statistic preceded by "B" applies to the second expansion module.

Display Expansion Modules Screen

To display the Expansion Modules screen, follow these steps:
Procedure

**Step 1** Press **Settings**.
**Step 2** Select **Status**.
**Step 3** Select **Expansion Modules**.
**Step 4** To exit the Expansion Modules screen, press **Exit**.

Expansion Module Items

**Table 46: Expansion Module Information**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link State</td>
<td>Overall expansion module status</td>
</tr>
<tr>
<td>RX Discarded Bytes</td>
<td>Number of bytes that are discarded due to errors</td>
</tr>
<tr>
<td>RX Length Err</td>
<td>Number of packets that are discarded due to improper length</td>
</tr>
<tr>
<td>RX Checksum Err</td>
<td>Number of packets that are discarded due to invalid checksum information</td>
</tr>
<tr>
<td>RX Invalid Message</td>
<td>Number of packets that are discarded because a message was invalid or unsupported</td>
</tr>
<tr>
<td>TX Retransmit</td>
<td>Number of packets that are retransmitted to the expansion module</td>
</tr>
<tr>
<td>TX Buffer Full</td>
<td>Number of packets that are discarded because the expansion module was not able to accept new messages</td>
</tr>
</tbody>
</table>

Call Statistics Screen

The Call Statistics screen displays counters statistics and voice-quality metrics in these ways:

- During call: You can view the call information by rapidly pressing the ? button twice.
- After the call: You can view the call information captured during the last call by displaying the Call Statistics screen.

**Note**

You can also remotely view the call statistics information by using a web browser to access the Streaming Statistics web page. This web page contains additional RTCP statistics not available on the phone. For more information about remote monitoring, see **Remote Monitoring**, on page 199.
A single call can have multiple voice streams, but data is captured for only the last voice stream. A voice stream is a packet stream between two endpoints. If one endpoint is put on hold, the voice stream stops even though the call is still connected. When the call resumes, a new voice packet stream begins, and the new call data overwrites the former call data.

**Display Call Statistics Screen**

To display the Call Statistics screen for information about the last voice stream, follow these steps:

**Procedure**

1. **Step 1** Press **Settings**.
2. **Step 2** Select **Status**.
3. **Step 3** Select **Call Statistics**.

**Call Statistics Items**

The following table explains the items displayed in the Call Statistics screen:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rcvr Codec</td>
<td>Type of voice stream received (RTP streaming audio from codec): G.729, G.711 Mu-law, G.711 A-law, or Lin16k.</td>
</tr>
<tr>
<td>Sender Codec</td>
<td>Type of voice stream transmitted (RTP streaming audio from codec): G.729, G.728/iLBC, G.711 Mu-law, G.711 A-law, or Lin16k.</td>
</tr>
<tr>
<td>Rcvr Size</td>
<td>Size of voice packets, in milliseconds, in the receiving voice stream (RTP streaming audio).</td>
</tr>
<tr>
<td>Sender Size</td>
<td>Size of voice packets, in milliseconds, in the transmitting voice stream.</td>
</tr>
<tr>
<td>Rcvr Packets</td>
<td>Number of RTP voice packets received since voice stream opened.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>This number is not necessarily identical to the number of RTP voice packets received since the call began because the call might have been placed on hold.</td>
</tr>
<tr>
<td>Sender Packets</td>
<td>Number of RTP voice packets transmitted since voice stream opened.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>This number is not necessarily identical to the number of RTP voice packets transmitted since the call began because the call might have been placed on hold.</td>
</tr>
<tr>
<td>Avg Jitter</td>
<td>Estimated average RTP packet jitter (dynamic delay that a packet encounters when going through the network) observed since the receiving voice stream opened.</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Max Jitter</td>
<td>Maximum jitter observed since the receiving voice stream opened.</td>
</tr>
<tr>
<td>Rcvr Discarded</td>
<td>Number of RTP packets in the receiving voice stream that have been discarded (such as bad packets or packets received too late).</td>
</tr>
<tr>
<td>Note</td>
<td>The phone discards payload type 19 comfort noise packets that by Cisco Gateways generate, which increment this counter.</td>
</tr>
<tr>
<td>Rcvr Lost Packets</td>
<td>Missing RTP packets (lost in transit).</td>
</tr>
<tr>
<td>Voice Quality Metrics</td>
<td></td>
</tr>
<tr>
<td>MOS LQK</td>
<td>Score that is an objective estimate of the mean opinion score (MOS) for listening quality (LQK) that rates from 5 (excellent) to 1 (bad). This score is based on audible concealment events due to frame loss in the preceding 8-second interval of the voice stream. For more information, see Voice Quality Monitoring, on page 239.</td>
</tr>
<tr>
<td>Note</td>
<td>The MOS LQK score can vary based on the type of codec that the Cisco Unified IP Phone uses.</td>
</tr>
<tr>
<td>Avg MOS LQK</td>
<td>Average MOS LQK score observed for the entire voice stream.</td>
</tr>
<tr>
<td>Min MOS LQK</td>
<td>Lowest MOS LQK score observed from start of the voice stream.</td>
</tr>
<tr>
<td>Max MOS LQK</td>
<td>Baseline or highest MOS LQK score observed from start of the voice stream. These codecs provide the following maximum MOS LQK score under normal conditions with no frame loss:</td>
</tr>
<tr>
<td></td>
<td>• G.711 gives 4.5.</td>
</tr>
<tr>
<td></td>
<td>• G.722 gives 4.5.</td>
</tr>
<tr>
<td></td>
<td>• G.728/iLBC gives 3.9.</td>
</tr>
<tr>
<td></td>
<td>• G.729 A/AB gives 3.8.</td>
</tr>
<tr>
<td>MOS LQK Version</td>
<td>Version of the Cisco proprietary algorithm used to calculate MOS LQK scores.</td>
</tr>
<tr>
<td>Cumulative Conceal Ratio</td>
<td>Total number of concealment frames divided by total number of speech frames received from start of the voice stream.</td>
</tr>
<tr>
<td>Interval Conceal Ratio</td>
<td>Ratio of concealment frames to speech frames in preceding 3-second interval of active speech. If using voice activity detection (VAD), a longer interval might be required to accumulate 3 seconds of active speech.</td>
</tr>
<tr>
<td>Max Conceal Ratio</td>
<td>Highest interval concealment ratio from start of the voice stream.</td>
</tr>
<tr>
<td>Conceal Secs</td>
<td>Number of seconds that have concealment events (lost frames) from the start of the voice stream (includes severely concealed seconds).</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Severely Conceal Secs</td>
<td>Number of seconds that have more than 5 percent concealment events (lost frames) from the start of the voice stream.</td>
</tr>
<tr>
<td>Latency (see note)</td>
<td>Estimate of the network latency, expressed in milliseconds. Represents a running average of the round-trip delay, measured when RTCP receiver report blocks are received.</td>
</tr>
</tbody>
</table>

**Note**

When the RTP Control Protocol is disabled, no data generates for this field and thus displays as 0.

## Test Tone

The Cisco Unified IP Phone supports a test tone, which allows you to troubleshoot echo on a call as well as to test low volume levels.

To use a test tone, you must:

- Enable the tone generator
- Create a test tone

### Enable Tone Generator

To enable the tone generator, follow these steps:

**Procedure**

**Step 1** Verify that the phone is unlocked.

When options are inaccessible for modification, a locked padlock icon appears on the configuration menus. When options are unlocked and accessible for modification, an unlocked padlock icon appears on these menus.

To unlock or lock options on the Settings menu, press **#** on the phone keypad. This action either locks or unlocks the options, depending on the previous state.

**Note** If a Settings Menu password has been provisioned, SIP phones present an “Enter password” prompt after you enter **#**. Make sure to lock options after you have made your changes.

**Caution** Do not press **##** to unlock options and then immediately press **###** again to lock options. The phone will interpret this sequence as **##**, which will reset the phone. To lock options after unlocking them, wait at least 10 seconds before you press **#** again.
Step 2  While offhook, press Help twice to invoke the Call Statistics screen, or press Settings > Status > Call Statistics to invoke the Call Statistics screen.

Step 3  Look for the Tone softkey.
When the Tone softkey is visible, the softkey remains enabled for as long as this Cisco Unified IP phone is registered with Cisco Unified Communications Manager.

Step 4  If the Tone softkey is present, proceed to Create Test Tone, on page 197.

Step 5  If the Tone softkey is not present, exit the Call Statistics screen and enter the Setting Menu.

Step 6  Press **3 on the phone keypad to enable (toggle) the Tone softkey.
Note  If you press **#**3 consecutively, with no pause, you will inadvertently reset the phone because of the **#** sequence.

Step 7  While offhook, press the Help button twice to invoke the Call Statistics screen, or press Settings > Status > Call Statistics to invoke the Call Statistics screen.

Step 8  Verify that the Tone softkey is present.
When the Tone softkey is visible, the softkey remains enabled for as long as this Cisco Unified IP Phone is registered with Cisco Unified Communications Manager.

---

Create Test Tone

Note  When measuring echo, make sure you first set the input and output levels to 0 dB gain/attenuation on the trunk. This is set for the gateway (in Cisco Unified Communications Manager for MGCP) or under IOS CLI for H.323 or SIP.

To create a test tone, follow these steps:

Procedure

Step 1  Place a call.

Step 2  After the call is established, press Help twice, or press Settings > Status > Call Statistics.
The Call Statistics screen and Tone softkey should appear.

Step 3  Press Tone.
The phone generates a 1004 Hz tone at -15 dBm.
  • For a good network connection, the tone sounds at the call destination only.
  • For a bad network connection, the phone generating the tone may receive echo from the destination phone.

Step 4  To stop the tone, end the call.
For information on interpreting the results of test tone for volume and echo, see Echo Analysis for Voice over IP.
Remote Monitoring Overview

Each Cisco Unified IP Phone has a web page from which you can view a variety of information about the phone, including:

- Device information
- Network configuration information
- Network statistics
- Device logs
- Streaming statistics

The Cisco Unified IP Phone does not support web access on its IPv6 address.

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.
You can also obtain much of this information directly from a phone. For more information, see Model Information, Status, and Statistics, on page 177.

For more information about troubleshooting the Cisco Unified IP Phone, see Troubleshooting and Maintenance, on page 217.

Access Web Page for Phone

To access the web page for a Cisco Unified IP Phone, perform these steps.

Note

If you cannot access the web page, it may be disabled. See Control Web Page Access, on page 201 for more information.

Procedure

Step 1 Obtain the IP address of the Cisco Unified IP Phone by using one of these methods:

a) Search for the phone in Cisco Unified Communications Manager by choosing Device > Phone. Phones registered with Cisco Unified Communications Manager display the IP address at the top of the Phone Configuration window.

b) On the phone, press the Settings button, choose Network Configuration, and then scroll to the IP Address option.

Step 2 Open a web browser and enter the following URL, where IP_address is the IP address of the Cisco Unified IP Phone:

http://<IP_address> or https://<IP_address> (depending on the protocol supported by the Cisco Unified IP Phone)

Cisco Unified IP Phone Web Page Information

The web page for a Cisco Unified IP Phone includes these hyperlinks:

• Device Information: Displays device settings and related information for the phone.

• Network Configuration: Displays network configuration information and information about other phone settings.

• Network Statistics: Includes the following hyperlinks, which provide information about network traffic:
  • Ethernet Information: Displays information about Ethernet traffic.
  • Access: Displays information about network traffic to and from the PC port on the phone.
  • Network: Displays information about network traffic to and from the network port on the phone.

• Device Logs: Includes the following hyperlinks, which provide information that you can use for troubleshooting:
• Console Logs: Includes hyperlinks to individual log files.
• Core Dumps: Includes hyperlinks to individual dump files.
• Status Messages
• Debug Display: Displays messages that might be useful to the Cisco TAC if you require assistance with troubleshooting.

• Streaming Statistics: Includes the Stream 1, Stream 2, Stream 3, Stream 4, and Stream 5 hyperlinks, which display a variety of streaming statistics.

Related Topics
- Device Information Area, on page 202
- Network Configuration Area, on page 203
- Network Statistics Area, on page 208
- Device Logs Area, on page 211
- Streaming Statistics, on page 211

Control Web Page Access

For security purposes, you may choose to prevent access to the web pages for a phone. If you do so, you will prevent access to the web pages that are described in this chapter and to the Cisco Unified Communications Manager User Options web pages.

You can enable or disable access to the web pages for an individual phone, a group of phones, or to all phones in the system.

To enable or disable access to the web pages for all phones on the system, choose System > Enterprise Parameters and select Enabled or Disabled from the Web Access drop-down menu.

To enable or disable access to the web pages for a group of phones, choose Device > Device Settings > Common Phone Profile to create a new phone profile or to update an existing phone profile, select Enabled or Disabled from the Web Access drop-down menu and select the common phone profile when you configure your phone.

To enable or disable access to the web pages for a phone, follow these steps from Cisco Unified Communications Manager Administration.

Procedure

Step 1 Choose Device > Phone.
Step 2 Specify the criteria to find the phone and click Find, or click Find to display a list of all phones.
Step 3 Click the device name to open the Phone Configuration window for the device.
Step 4 Scroll down to the Product Specific Configuration section. From the Web Access drop-down list box, choose Disabled if you want to disable the phone and choose Enabled if you want to enable the phone.
Step 5 Click Update.

Note Some features, such as Cisco Quality Report Tool, do not function properly without access to the phone web pages. Disabling web access also affects any serviceability application that relies on web access, such as CiscoWorks.
Cisco Unified IP Phone and HTTP or HTTPS Protocols

The Cisco Unified IP Phone can be configured to use:

- HTTPS protocol only
- HTTP or HTTPS protocols

If your Cisco Unified IP Phone is configured to use the HTTP or HTTPS protocols, use `http://<IP_address>` or `https://<IP_address>` for phone web access.

If your Cisco Unified IP Phone is configured to use only HTTPS protocol, use `https://<IP_address>` for phone web access.

Device Information Area

The Device Information area on a phone web page displays device settings and related information for the phone. The following table describes these items.

To display the Device Information area, access the web page for the phone as described in Access Web Page for Phone, on page 200, and then click the Device Information hyperlink.

Table 48: Device Information Area Items

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>Media Access Control (MAC) address of the phone</td>
</tr>
<tr>
<td>Host Name</td>
<td>Unique, fixed name that is automatically assigned to the phone based on its MAC address</td>
</tr>
<tr>
<td>Phone DN</td>
<td>Directory number assigned to the phone</td>
</tr>
<tr>
<td>App Load ID</td>
<td>Identifier of the firmware running on the phone</td>
</tr>
<tr>
<td>Boot Load ID</td>
<td>Identifier of the factory-installed load running on the phone</td>
</tr>
<tr>
<td>Version</td>
<td>Version of the firmware running on the phone</td>
</tr>
<tr>
<td>Expansion Module 1</td>
<td>Phone load ID for the first Cisco Unified IP Phone Expansion Module.</td>
</tr>
<tr>
<td>Expansion Module 2</td>
<td>Phone load ID for the second Cisco Unified IP Phone Expansion Module.</td>
</tr>
<tr>
<td>Hardware Revision</td>
<td>Revision value of the phone hardware</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Serial number of the phone</td>
</tr>
<tr>
<td>Model Number</td>
<td>Model number of the phone</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Message Waiting</td>
<td>Indicator of a voice message on any line of this phone</td>
</tr>
</tbody>
</table>
| UDI             | Displays the following Cisco Unique Device Identifier (UDI) information about the phone:  
  • Device Type: Indicates hardware type. For example, phone displays for all phone models.  
  • Device Description: Displays the name of the phone that is associated with the indicated model type.  
  • Product Identifier: Specifies the phone model.  
  • Version Identifier: Represents the hardware version of the phone. The Version Identifier field might display blank if using an older model Cisco Unified IP Phone because the hardware does not provide this information.  
  • Serial Number: Displays the unique serial number of the phone.  
| Time            | Time obtained from the Date/Time Group in Cisco Unified Communications Manager to which the phone belongs.                               |
| Time Zone       | Time zone obtained from the Date/Time Group in Cisco Unified Communications Manager to which the phone belongs.                           |
| Date            | Date obtained from the Date/Time Group in Cisco Unified Communications Manager to which the phone belongs.                               |
| LLDP: PC Port   | Indicates whether Link Layer Discovery Protocol (LLDP) is enabled on the PC port.                                                             |
| LLDP-MED: SW Port| Indicates whether Link Layer Discovery Protocol Media Endpoint Discovery (LLDP-MED) is enabled on the switch port.                         |

**Network Configuration Area**

The Network Configuration area on a phone web page displays network configuration information and information about other phone settings. The following table describes this information.

You can view and set many of these items from the Network Configuration Menu and the Device Configuration Menu on the Cisco Unified IP Phone. For more information, see Features, Templates, Services, and Users, on page 123.

To display the Network Configuration area, access the web page for the phone as described in the Access Web Page for Phone, on page 200, and then click the Network Configuration hyperlink.
<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Server</td>
<td>IP address of the Dynamic Host Configuration Protocol (DHCP) server from which the phone obtains its IP address.</td>
</tr>
<tr>
<td>BOOTP Server</td>
<td>Indicates whether the phone obtains its configuration from a Bootstrap Protocol (BootP) server.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Media Access Control (MAC) address of the phone.</td>
</tr>
<tr>
<td>Host Name</td>
<td>Host name that the DHCP server assigned to the phone.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Name of the Domain Name System (DNS) domain in which the phone resides.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Internet Protocol (IP) address of the phone.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Subnet mask used by the phone.</td>
</tr>
<tr>
<td>TFTP Server 1</td>
<td>Primary Trivial File Transfer Protocol (TFTP) server used by the phone.</td>
</tr>
<tr>
<td>Default Router 1 to 5</td>
<td>Default router used by the phone (Default Router 1) and optional backup routers (Default Router 2–5).</td>
</tr>
<tr>
<td>DNS Server 1 to 5</td>
<td>Primary Domain Name System (DNS) server (DNS Server 1) and optional backup DNS servers (DNS Server 2–5) used by the phone.</td>
</tr>
<tr>
<td>Operational VLAN ID</td>
<td>Auxiliary Virtual Local Area Network (VLAN) configured on a Cisco Catalyst switch in which the phone is a member.</td>
</tr>
<tr>
<td>Admin. VLAN ID</td>
<td>Auxiliary VLAN in which the phone is a member.</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Unified CM 1 to 5 | Host names or IP addresses, in prioritized order, of the Cisco Unified Communications Manager servers with which the phone can register. An item can also show the IP address of an SRST router that is capable of providing limited Cisco Unified Communications Manager functionality, if such a router is available. For an available server, an item will show the Cisco Unified Communications Manager server IP address and one of the following states:  
  - Active: Cisco Unified Communications Manager server from which the phone is currently receiving call-processing services.  
  - Standby: Cisco Unified Communications Manager server to which the phone switches if the current server becomes unavailable.  
  - Blank: No current connection to this Cisco Unified Communications Manager server.  
  An item may also include the Survivable Remote Site Telephony (SRST) designation, which identifies an SRST router capable of providing Cisco Unified Communications Manager functionality with a limited feature set. This router assumes control of call processing if all other Cisco Unified Communications Manager servers become unreachable. The SRST Cisco Unified Communications Manager always appears last in the list of servers, even if it is active. You configure the SRST router address in the Device Pool section in Cisco Unified Communications Manager Configuration window. |
| Information URL   | URL of the help text that appears on the phone.                                                                                                                                                                                                                                                                                    |
| Directories URL   | URL of the server from which the phone obtains directory information.                                                                                                                                                                                                         |
| Messages URL      | URL of the server from which the phone obtains message services.                                                                                                                                                                                                          |
| Services URL      | URL of the server from which the phone obtains Cisco Unified IP Phone services.                                                                                                                                                                                                  |
| DHCP Enabled      | Indicates whether DHCP is being used by the phone.                                                                                                                                                                                                                         |
| DHCP Address Released | Indicates the setting of the DHCP Address Released option on the phone Network Configuration menu.                                                                                      |
| Alternate TFTP     | Indicates whether the phone is using an alternative TFTP server.                                                                                                                                                                                                          |
| Idle URL          | URL that the phone displays when the phone has not been used for the time specified by Idle URL Time, and no menu is open.                                                                                                                                                     |
| Idle URL Time     | Number of seconds that the phone has not been used and no menu is open before the XML service specified by Idle URL is activated.                                                                                                                                          |
| Proxy Server URL  | URL of proxy server, which makes HTTP requests to non-local host addresses on behalf of the phone HTTP client and provides responses from the non-local host to the phone HTTP client.                                                                                              |
### Network Configuration Area

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication URL</td>
<td>URL that the phone uses to validate requests made to the phone web server.</td>
</tr>
<tr>
<td>SW Port Configuration</td>
<td>Speed and duplex of the switch port, where:</td>
</tr>
<tr>
<td></td>
<td>• A = Auto Negotiate</td>
</tr>
<tr>
<td></td>
<td>• 10H = 10-BaseT/half duplex</td>
</tr>
<tr>
<td></td>
<td>• 10F = 10-BaseT/full duplex</td>
</tr>
<tr>
<td></td>
<td>• 100H = 100-BaseT/half duplex</td>
</tr>
<tr>
<td></td>
<td>• 100F = 100-BaseT/full duplex</td>
</tr>
<tr>
<td></td>
<td>• 1000H = 1000-BaseT/half duplex</td>
</tr>
<tr>
<td></td>
<td>• 1000F = 1000-BaseT/full duplex</td>
</tr>
<tr>
<td></td>
<td>• No Link = No connection to the switch port</td>
</tr>
<tr>
<td>PC Port Configuration</td>
<td>Speed and duplex of the switch port, where:</td>
</tr>
<tr>
<td></td>
<td>• A = Autonegotiate</td>
</tr>
<tr>
<td></td>
<td>• 10H = 10-BaseT/half duplex</td>
</tr>
<tr>
<td></td>
<td>• 10F = 10-BaseT/full duplex</td>
</tr>
<tr>
<td></td>
<td>• 100H = 100-BaseT/half duplex</td>
</tr>
<tr>
<td></td>
<td>• 100F = 100-BaseT/full duplex</td>
</tr>
<tr>
<td></td>
<td>• 1000H = 1000-BaseT/half duplex</td>
</tr>
<tr>
<td></td>
<td>• 1000F = 1000-BaseT/full duplex</td>
</tr>
<tr>
<td></td>
<td>• No Link = No connection to the PC port</td>
</tr>
</tbody>
</table>

To configure the setting on multiple phones simultaneously, configure the Remote Port Configuration in the Enterprise Phone Configuration (System > Enterprise Phone Configuration).

**Note**  If the ports are configured for Remote Port Configuration in Unified CM, the data cannot be changed on the phone.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TFTP Server 2</td>
<td>Backup TFTP server that the phone uses if the primary TFTP server is unavailable.</td>
</tr>
<tr>
<td>User Locale</td>
<td>User locale associated with the phone user. Identifies a set of detailed information to support users, including language, font, date and</td>
</tr>
<tr>
<td></td>
<td>time formatting, and alphanumeric keyboard text information.</td>
</tr>
<tr>
<td>Network Locale</td>
<td>Network locale associated with the phone user. Identifies a set of detailed information to support the phone in a specific location, including</td>
</tr>
<tr>
<td></td>
<td>definitions of the tones and cadences used by the phone.</td>
</tr>
<tr>
<td>Headset enabled</td>
<td>Indicates whether the Headset button is enabled on the phone.</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>User Locale Version</td>
<td>Version of the user locale loaded on the phone.</td>
</tr>
<tr>
<td>Network Locale Version</td>
<td>Version of the network locale loaded on the phone.</td>
</tr>
<tr>
<td>PC Port Disabled</td>
<td>Indicates whether the PC port on the phone is enabled or disabled.</td>
</tr>
<tr>
<td>Speaker Enabled</td>
<td>Indicates whether the speakerphone is enabled on the phone.</td>
</tr>
<tr>
<td>GARP Enabled</td>
<td>Indicates whether the phone learns MAC addresses from Gratuitous ARP responses.</td>
</tr>
<tr>
<td>Video Capability Enabled</td>
<td>Indicates whether the phone can participate in video calls when connected to an appropriately equipped PC.</td>
</tr>
<tr>
<td>Voice VLAN Enabled</td>
<td>Indicates whether the phone allows a device attached to the PC port to access the Voice VLAN.</td>
</tr>
<tr>
<td>Auto Line Select</td>
<td>Indicates whether the phone shifts the call focus to incoming calls on all lines.</td>
</tr>
<tr>
<td>DSCP for Call Control</td>
<td>DSCP IP classification for call control signaling.</td>
</tr>
<tr>
<td>DSCP for Configuration</td>
<td>DSCP IP classification for any phone configuration transfer.</td>
</tr>
<tr>
<td>DSCP for Services</td>
<td>DSCP IP classification for phone-based services.</td>
</tr>
<tr>
<td>Security Mode</td>
<td>Displays the security mode that is set for the phone.</td>
</tr>
<tr>
<td>Web Access Enabled</td>
<td>Indicates whether web access is enabled (Yes) or disabled (No) for the phone.</td>
</tr>
<tr>
<td>Span to PC Port</td>
<td>Indicates whether the phone will forward packets transmitted and received on the network port to the access port.</td>
</tr>
<tr>
<td>PC VLAN</td>
<td>VLAN used to identify and remove 802.1P/Q tags from packets sent to the PC.</td>
</tr>
<tr>
<td>Forwarding Delay</td>
<td>Indicates whether the internal switch begins forwarding packets between the PC port and switched port on the phone when the phone becomes active.</td>
</tr>
<tr>
<td>CDP: PC Port</td>
<td>Indicates whether CDP is supported on the PC port.</td>
</tr>
<tr>
<td>CDP: SW Port</td>
<td>Indicates whether CDP is supported on the switch port.</td>
</tr>
<tr>
<td>LLDP-MED: SW Port</td>
<td>Indicates whether Link Layer Discovery Protocol Media Endpoint Discovery (LLDP-MED) is enabled on the switch port.</td>
</tr>
<tr>
<td>LLDP: PC Port</td>
<td>Indicates whether Link Layer Discovery Protocol (LLDP) is enabled on the PC port.</td>
</tr>
<tr>
<td>LLDP Asset ID</td>
<td>Identifies the asset ID assigned to the phone for inventory management.</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Wireless Headset Hookswitch Control</td>
<td>Enables users to receive notifications of incoming calls and answer or end calls while working in a wireless environment.</td>
</tr>
<tr>
<td>LLDP Power Priority</td>
<td>Advertises the phone power priority to the switch, enabling the switch to appropriately provide power to the phones. Settings include: • Unknown (default) • Low • High • Critical</td>
</tr>
</tbody>
</table>

**Network Statistics Area**

These network statistics areas on a phone web page provide information about network traffic on the phone:

- Ethernet Information area: Displays information about Ethernet traffic.
- Access area: Displays information about network traffic to and from the PC port on the phone.
- Network area: Displays information about network traffic to and from the network port on the phone.

To display a network statistics area, access the web page for the phone as described in Access Web Page for Phone, on page 200, and then click the Ethernet Information, Access, or Network hyperlink.

**Related Topics**

- Ethernet Information Area, on page 208
- Access and Network Areas, on page 209

**Ethernet Information Area**

*Table 50: Ethernet Information Area Items*

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tx Frames</td>
<td>Total number of packets that the phone transmits</td>
</tr>
<tr>
<td>Tx broadcast</td>
<td>Total number of broadcast packets that the phone transmits</td>
</tr>
<tr>
<td>Tx multicast</td>
<td>Total number of multicast packets that the phone transmits</td>
</tr>
<tr>
<td>Tx unicast</td>
<td>Total number of unicast packets that the phone transmits</td>
</tr>
<tr>
<td>Rx Frames</td>
<td>Total number of packets the phone receives</td>
</tr>
</tbody>
</table>
### Access and Network Areas

**Table 51: Access Area and Network Area Items**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rx broadcast</td>
<td>Total number of broadcast packets the phone receives</td>
</tr>
<tr>
<td>Rx multicast</td>
<td>Total number of multicast packets the phone receives</td>
</tr>
<tr>
<td>Rx unicast</td>
<td>Total number of unicast packets the phone receives</td>
</tr>
<tr>
<td>RxPacketNoDes</td>
<td>Total number of shed packets that a missing Direct Memory Access (DMA) descriptor causes</td>
</tr>
<tr>
<td>Rx totalPkt</td>
<td>Total number of packets that the phone receives</td>
</tr>
<tr>
<td>Rx crcErr</td>
<td>Total number of packets that are received with CRC failed</td>
</tr>
<tr>
<td>Rx alignErr</td>
<td>Total number of packets between 64 and 1522 bytes in length that are received with a bad Frame Check Sequence (FCS)</td>
</tr>
<tr>
<td>Rx multicast</td>
<td>Total number of multicast packets that the phone receives</td>
</tr>
<tr>
<td>Rx broadcast</td>
<td>Total number of broadcast packets that the phone receives</td>
</tr>
<tr>
<td>Rx unicast</td>
<td>Total number of unicast packets that the phone receives</td>
</tr>
<tr>
<td>Rx shortErr</td>
<td>Total number of FCS error packets or Align error packets that are received with less than 64 bytes in size</td>
</tr>
<tr>
<td>Rx shortGood</td>
<td>Total number of good packets that the phone receives are less than 64 bytes size</td>
</tr>
<tr>
<td>Rx longGood</td>
<td>Total number of good packets that the phone receives are greater than 1522 bytes in size</td>
</tr>
<tr>
<td>Rx longErr</td>
<td>Total number of FCS error packets or Align error packets that the phone receives that are greater than 1522 bytes in size</td>
</tr>
<tr>
<td>Rx size64</td>
<td>Total number of packets received, including bad packets, that are between 0 and 64 bytes in size</td>
</tr>
<tr>
<td>Rx size65to127</td>
<td>Total number of packets that the phone receives, including bad packets, that are between 65 and 127 bytes in size</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Rx size128to255</td>
<td>Total number of packets that the phone receives, including bad packets, that are between 128 and 255 bytes in size</td>
</tr>
<tr>
<td>Rx size256to511</td>
<td>Total number of packets that the phone receives, including bad packets, that are between 256 and 511 bytes in size</td>
</tr>
<tr>
<td>Rx size512to1023</td>
<td>Total number of packets that the phone receives, including bad packets, that are between 512 and 1023 bytes in size</td>
</tr>
<tr>
<td>Rx size1024to1518</td>
<td>Total number of packets that the phone receives, including bad packets, that are between 1024 and 1518 bytes in size</td>
</tr>
<tr>
<td>Rx tokenDrop</td>
<td>Total number of packets dropped due to lack of resources (for example, FIFO overflow)</td>
</tr>
<tr>
<td>Tx excessDefer</td>
<td>Total number of packets delayed from transmitting due to medium being busy</td>
</tr>
<tr>
<td>Tx lateCollision</td>
<td>Number of times that collisions occurred later than 512 bit times after the start of packet transmission</td>
</tr>
<tr>
<td>Tx totalGoodPkt</td>
<td>Total number of good packets (multicast, broadcast, and unicast) that the phone receives</td>
</tr>
<tr>
<td>Tx Collisions</td>
<td>Total number of collisions that occurred while a packet was being transmitted</td>
</tr>
<tr>
<td>Tx excessLength</td>
<td>Total number of packets not transmitted because the packet experienced 16 transmission attempts</td>
</tr>
<tr>
<td>Tx broadcast</td>
<td>Total number of broadcast packets that a phone transmits</td>
</tr>
<tr>
<td>Tx multicast</td>
<td>Total number of multicast packets that a phone transmits</td>
</tr>
<tr>
<td>Neighbor Device ID</td>
<td>Identifier of a device connected to this port</td>
</tr>
<tr>
<td>Neighbor IP Address</td>
<td>IP address of the neighbor device</td>
</tr>
<tr>
<td>Neighbor Port</td>
<td>Neighbor device port to which the phone is connected</td>
</tr>
<tr>
<td>LLDP FramesOutTotal</td>
<td>Total number of LLDP frames sent out from the phone</td>
</tr>
<tr>
<td>LLDP AgeoutsTotal</td>
<td>Total number of LLDP frames that have been time out in cache</td>
</tr>
<tr>
<td>LLDP FramesDiscardedTotal</td>
<td>Total number of LLDP frames that are discarded when any of the mandatory TLVs is missing or out of order or contains out of range string length</td>
</tr>
<tr>
<td>LLDP FramesInErrorsTotal</td>
<td>Total number of LLDP frames that received with one or more detectable errors</td>
</tr>
<tr>
<td>LLDP FramesInTotal</td>
<td>Total number of LLDP frames that a phone receives</td>
</tr>
</tbody>
</table>
### Device Logs Area

The Device Logs area on a phone web page provides information that you can use to help monitor and troubleshoot the phone.

- **Console Logs:** Includes hyperlinks to individual log files. The console log files include debug and error messages received on the phone.

- **Core Dumps:** Includes hyperlinks to individual dump files.

- **Status Messages area:** Displays up to the 10 most recent status messages that the phone has generated since it was last powered up. You can also see this information from the Status Messages screen on the phone. Status Messages Screen, on page 179 describes the status messages that can appear.

  To display the Status Messages, access the web page for the phone as described in Access Web Page for Phone, on page 200, and then click the Status Messages hyperlink.

- **Debug Display area:** Displays debug messages that might be useful to Cisco TAC if you require assistance with troubleshooting.

### Streaming Statistics

A Cisco Unified IP Phone can stream information to and from up to three devices simultaneously. A phone streams information when it is on a call or running a service that sends or receives audio or data.

The streaming statistics areas on a phone web page provide information about the streams. Most calls use only one stream (Stream 1), but some calls use two or three streams. For example, a barged call uses Stream 1 and Stream 2.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LLDP TLVDiscardedTotal</td>
<td>Total number of LLDP TLVs that are discarded</td>
</tr>
<tr>
<td>LLDP TLVUnrecognizedTotal</td>
<td>Total number of LLDP TLVs that are not recognized on the phone</td>
</tr>
<tr>
<td>CDP Neighbor Device ID</td>
<td>Identifier of a device connected to this port discovered by CDP protocol</td>
</tr>
<tr>
<td>CDP Neighbor IP Address</td>
<td>IP address of the neighbor device discovered by CDP protocol</td>
</tr>
<tr>
<td>CDP Neighbor Port</td>
<td>Neighbor device port to which the phone is connected discovered by CDP protocol</td>
</tr>
<tr>
<td>LLDP Neighbor Device ID</td>
<td>Identifier of a device connected to this port discovered by LLDP protocol</td>
</tr>
<tr>
<td>LLDP Neighbor IP Address</td>
<td>IP address of the neighbor device discovered by LLDP protocol</td>
</tr>
<tr>
<td>LLDP Neighbor Port</td>
<td>Neighbor device port to which the phone is connected discovered by LLDP protocol</td>
</tr>
</tbody>
</table>
To display a Streaming Statistics area, access the web page for the phone as described in Access Web Page for Phone, on page 200, and then click the Stream 1, the Stream 2, or the Stream 3 hyperlink (Cisco Unified IP Phones 7975G, 7965G, and 7945G also include Stream 4 and Stream 5 hyperlinks).

The following table describes the items in the Streaming Statistics areas.

**Table 52: Streaming Statistics Area Items**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Address</td>
<td>IP address and UDP port of the destination of the stream.</td>
</tr>
<tr>
<td>Local Address</td>
<td>IP address and UDP port of the phone.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Internal time stamp indicating when Cisco Unified Communications Manager requested that the phone start transmitting packets.</td>
</tr>
<tr>
<td>Stream Status</td>
<td>Indication of whether streaming is active.</td>
</tr>
<tr>
<td>Host Name</td>
<td>Unique, fixed name that is automatically assigned to the phone based on its MAC address.</td>
</tr>
<tr>
<td>Sender Packets</td>
<td>Total number of RTP data packets transmitted by the phone since starting this connection. The value is 0 if the connection is set to receive only mode.</td>
</tr>
<tr>
<td>Sender Octets</td>
<td>Total number of payload octets transmitted in RTP data packets by the phone since starting this connection. The value is 0 if the connection is set to receive only mode.</td>
</tr>
<tr>
<td>Sender Codec</td>
<td>Type of audio encoding used for the transmitted stream.</td>
</tr>
<tr>
<td>Sender Reports Sent</td>
<td>Number of times the RTCP Sender Reports have been sent.</td>
</tr>
<tr>
<td>Sender Report Time Sent</td>
<td>Internal time stamp indicating when a RTCP Sender Report was sent.</td>
</tr>
<tr>
<td>Rcvr Lost Packets</td>
<td>Total number of RTP data packets that have been lost since starting receiving data on this connection. Defined as the number of expected packets less the number of packets actually received, where the number of received packets includes any that are late or duplicate. The value displays as 0 if the connection was set to send-only mode.</td>
</tr>
<tr>
<td>Avg Jitter</td>
<td>Estimate of mean deviation of the RTP data packet inter-arrival time, measured in milliseconds. The value displays as 0 if the connection was set to send-only mode.</td>
</tr>
<tr>
<td>Rcvr Codec</td>
<td>Type of audio encoding used for the received stream.</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Rcvr Reports Sent</td>
<td>Number of times the RTCP Receiver Reports have been sent.</td>
</tr>
<tr>
<td>(See Note)</td>
<td></td>
</tr>
<tr>
<td>Rcvr Report Time Sent</td>
<td>Internal time stamp indicating when a RTCP Receiver Report was sent.</td>
</tr>
<tr>
<td>(See Note)</td>
<td></td>
</tr>
<tr>
<td>Rcvr Packets</td>
<td>Total number of RTP data packets received by the phone since starting</td>
</tr>
<tr>
<td></td>
<td>receiving data on this connection. Includes packets received from different</td>
</tr>
<tr>
<td></td>
<td>sources if this is a multicast call. The value displays as 0 if the</td>
</tr>
<tr>
<td></td>
<td>connection was set to send-only mode.</td>
</tr>
<tr>
<td>Rcvr Octets</td>
<td>Total number of payload octets received in RTP data packets by the device</td>
</tr>
<tr>
<td></td>
<td>since starting reception on the connection. Includes packets received from</td>
</tr>
<tr>
<td></td>
<td>different sources if this is a multicast call. The value displays as 0 if</td>
</tr>
<tr>
<td></td>
<td>the connection was set to send-only mode.</td>
</tr>
<tr>
<td>MOS LQK</td>
<td>Score that is an objective estimate of the mean opinion score (MOS) for</td>
</tr>
<tr>
<td></td>
<td>listening quality (LQK) that rates from 5 (excellent) to 1 (bad). This</td>
</tr>
<tr>
<td></td>
<td>score is based on audible concealment events due to frame loss in the</td>
</tr>
<tr>
<td></td>
<td>preceding 8-second interval of the voice stream. For more information, see</td>
</tr>
<tr>
<td></td>
<td>Voice Quality Monitoring, on page 239.</td>
</tr>
<tr>
<td>Note</td>
<td>The MOS LQK score can vary based on the type of codec that the Cisco</td>
</tr>
<tr>
<td></td>
<td>Unified IP Phone uses.</td>
</tr>
<tr>
<td>Avg MOS LQK</td>
<td>Average MOS LQK score observed for the entire voice stream.</td>
</tr>
<tr>
<td>Min MOS LQK</td>
<td>Lowest MOS LQK score observed from start of the voice stream.</td>
</tr>
<tr>
<td>Max MOS LQK</td>
<td>Baseline or highest MOS LQK score observed from start of the voice stream.</td>
</tr>
<tr>
<td></td>
<td>These codecs provide the following maximum MOS LQK score under normal</td>
</tr>
<tr>
<td></td>
<td>conditions with no frame loss:</td>
</tr>
<tr>
<td></td>
<td><strong>For Cisco Unified IP Phone 7975G, 7965G, and 7945G:</strong></td>
</tr>
<tr>
<td></td>
<td>• G.711 gives 4.5.</td>
</tr>
<tr>
<td></td>
<td>• G.722 gives 4.5.</td>
</tr>
<tr>
<td></td>
<td>• G.728/iLBC gives 3.9.</td>
</tr>
<tr>
<td></td>
<td>• G.729 A/AB gives 3.8.</td>
</tr>
<tr>
<td></td>
<td><strong>For Cisco Unified IP Phone 7971G-GE and 7970G:</strong></td>
</tr>
<tr>
<td></td>
<td>• G.711 gives 4.5</td>
</tr>
<tr>
<td></td>
<td>• G.729 A/AB gives 3.7</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>MOS LQK Version</td>
<td>Version of the Cisco proprietary algorithm used to calculate MOS LQK scores.</td>
</tr>
<tr>
<td>Cumulative Conceal Ratio</td>
<td>Total number of concealment frames divided by total number of speech frames received from start of the voice stream.</td>
</tr>
<tr>
<td>Interval Conceal Ratio</td>
<td>Ratio of concealment frames to speech frames in preceding 3-second interval of active speech. If using voice activity detection (VAD), a longer interval might be required to accumulate 3 seconds of active speech.</td>
</tr>
<tr>
<td>Max Conceal Ratio</td>
<td>Highest interval concealment ratio from start of the voice stream.</td>
</tr>
<tr>
<td>Conceal Secs</td>
<td>Number of seconds that have concealment events (lost frames) from the start of the voice stream (includes severely concealed seconds).</td>
</tr>
<tr>
<td>Severely Conceal Secs</td>
<td>Number of seconds that have more than 5 percent concealment events (lost frames) from the start of the voice stream.</td>
</tr>
<tr>
<td>Latency (See Note)</td>
<td>Estimate of the network latency, expressed in milliseconds. Represents a running average of the round-trip delay, measured when RTCP receiver report blocks are received.</td>
</tr>
<tr>
<td>Max Jitter</td>
<td>Maximum value of instantaneous jitter, in milliseconds.</td>
</tr>
<tr>
<td>Sender Size</td>
<td>RTP packet size, in milliseconds, for the transmitted stream.</td>
</tr>
<tr>
<td>Sender Reports Received (See Note)</td>
<td>Number of times RTCP Sender Reports have been received.</td>
</tr>
<tr>
<td>Sender Report Time Received (See Note)</td>
<td>Last time at which an RTCP Sender Report was received.</td>
</tr>
<tr>
<td>Rcvr Size</td>
<td>RTP packet size, in milliseconds, for the received stream.</td>
</tr>
<tr>
<td>Rcvr Discarded</td>
<td>RTP packets received from network but discarded from jitter buffers.</td>
</tr>
<tr>
<td>Rcvr Reports Received (See Note)</td>
<td>Number of times RTCP Receiver Reports have been received.</td>
</tr>
<tr>
<td>Rcvr Report Time Received (See Note)</td>
<td>Last time at which an RTCP Receiver Report was received.</td>
</tr>
</tbody>
</table>

**Voice Quality Metrics**
Score that is an objective estimate of the mean opinion score (MOS) for listening quality (LQK) that rates from 5 (excellent) to 1 (bad). This score is based on audible concealment events due to frame loss in the preceding 8-second interval of the voice stream. For more information, see Voice Quality Monitoring, on page 239.

**Note**  
The MOS LQK score can vary based on the type of codec that the Cisco Unified IP Phone uses.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MOS LQK</td>
<td>Score that is an objective estimate of the mean opinion score (MOS) for listening quality (LQK) that rates from 5 (excellent) to 1 (bad). This score is based on audible concealment events due to frame loss in the preceding 8-second interval of the voice stream. For more information, see Voice Quality Monitoring, on page 239.</td>
</tr>
<tr>
<td>Avg MOS LQK</td>
<td>Average MOS LQK score observed for the entire voice stream.</td>
</tr>
<tr>
<td>Min MOS LQK</td>
<td>Lowest MOS LQK score observed from start of the voice stream.</td>
</tr>
<tr>
<td>Max MOS LQK</td>
<td>Baseline or highest MOS LQK score observed from start of the voice stream.</td>
</tr>
<tr>
<td></td>
<td>These codecs provide the following maximum MOS LQK score under normal conditions with no frame loss:</td>
</tr>
<tr>
<td></td>
<td>For Cisco Unified IP Phone 7975G, 7965G, and 7945G:</td>
</tr>
<tr>
<td></td>
<td>• G.711 gives 4.5.</td>
</tr>
<tr>
<td></td>
<td>• G.722 gives 4.5.</td>
</tr>
<tr>
<td></td>
<td>• G.728/iLBC gives 3.9.</td>
</tr>
<tr>
<td></td>
<td>• G.729 A/AB gives 3.8.</td>
</tr>
<tr>
<td></td>
<td>For Cisco Unified IP Phone 7971G-GE and 7970G:</td>
</tr>
<tr>
<td></td>
<td>• G.711 gives 4.5</td>
</tr>
<tr>
<td></td>
<td>• G.729 A/AB gives 3.7</td>
</tr>
<tr>
<td>MOS LQK Version</td>
<td>Version of the Cisco proprietary algorithm used to calculate MOS LQK scores.</td>
</tr>
<tr>
<td>Cmtlve Conceal Ratio</td>
<td>Total number of concealment frames divided by total number of speech frames received from start of the voice stream.</td>
</tr>
<tr>
<td>Interval Conceal Ratio</td>
<td>Ratio of concealment frames to speech frames in preceding 3-second interval of active speech. If using voice activity detection (VAD), a longer interval might be required to accumulate 3 seconds of active speech.</td>
</tr>
<tr>
<td>Max Conceal Ratio</td>
<td>Highest interval concealment ratio from start of the voice stream.</td>
</tr>
<tr>
<td>Conceal Secs</td>
<td>Number of seconds that have concealment events (lost frames) from the start of the voice stream (includes severely concealed seconds).</td>
</tr>
<tr>
<td>Severely Conceal Secs</td>
<td>Number of seconds that have more than 5 percent concealment events (lost frames) from the start of the voice stream.</td>
</tr>
</tbody>
</table>
When the RTP Control Protocol is disabled, no data generates for this field and thus displays as 0.

**Related Topics**

- Cisco Unified IP Phone Settings, on page 61
- Features, Templates, Services, and Users, on page 123
- Call Statistics Screen, on page 193
- Voice Quality Monitoring, on page 239
Troubleshooting and Maintenance Overview

This chapter provides information that can assist you in troubleshooting problems with your Cisco Unified IP Phone or with your IP telephony network. It also explains how to clean and maintain your phone.

For additional troubleshooting information, see the Using the 79xx Status Information For Troubleshooting tech note. This document is available to registered Cisco.com users at this URL:

Troubleshooting

This section includes the following topics:

Startup Problems

After installing a Cisco Unified IP Phone into your network and adding it to Cisco Unified Communications Manager, the phone should start up as described in Phone Startup Process, on page 57. If the phone does not start up properly, see the following sections for troubleshooting information:

Cisco Unified IP Phone Does Not Go Through Normal Startup Process

**Problem**

When you connect a Cisco Unified IP Phone into the network port, the phone should go through the normal startup process, and the LCD screen should display information.
**Cause**

If the phone does not go through the startup process, the cause may be faulty cables, bad connections, network outages, or lack of power. Or, the phone may not be functional.

**Solution**

To determine whether the phone is faulty, follow these suggestions to systematically eliminate these other potential problems:

1. **Verify that the network port is functional:**
   - Exchange the Ethernet cables with cables that you know are functional.
   - Connect a operational phone to this network port to verify the port is active.
   - Replace an operational phone with the nonoperational phone.
   - Connect the nonoperational phone directly to the port on the switch, eliminating the patch panel connection in the office.

2. **Verify that the phone is receiving power:**
   - If you are using external power, verify that the electrical outlet is functional.
   - If you are using in-line power, plug the phone into an electrical outlet using the external power supply.
   - If you are using the external power supply, switch the power supply with a unit that you know works.
   - Make sure that the phone is connected to a switch that supports IEEE 802.3af Class 3 (15.4 W in-line power at the switch port).

3. If the phone still does not start up properly, power up the phone with the handset off-hook. When the phone is powered up in this way, it attempts to launch a backup software image.

4. If the phone still does not start up properly, perform a factory reset of the phone.

If after attempting these solutions, the LCD screen on the Cisco Unified IP Phone does not display any characters after at least five minutes, contact a Cisco technical support representative for additional assistance.

**Related Topics**

- Phone Startup Process, on page 57
- Cisco Unified IP Phone Power, on page 31
- Factory Reset, on page 237

**Cisco Unified IP Phone Does Not Register with Cisco Unified Communications Manager**

If the phone proceeds past the first stage of the startup process (LED buttons flashing on and off) but continues to cycle through the messages displaying on the LCD screen, the phone is not starting up properly. The phone cannot successfully start up unless it is connected to the Ethernet network and it has registered with a Cisco Unified Communications Manager server.

These sections can assist you in determining the reason the phone is unable to start up properly:
Phone Displays Error Messages

**Problem**
Status messages display errors during startup.

**Solution**
As the phone cycles through the startup process, you can access status messages that might provide you with information about the cause of a problem. See Status Messages Screen, on page 179 for instructions about accessing status messages and for a list of potential errors, their explanations, and their solutions.

Phone Cannot Connect to TFTP Server or to Cisco Unified Communications Manager

**Problem**
If the network is down between the phone and either the TFTP server or Cisco Unified Communications Manager, the phone cannot start up properly.

**Solution**
Ensure that the network is currently running.

TFTP Server Settings

**Problem**
The TFTP server settings may not be correct.

**Solution**
Check the TFTP settings. See Check TFTP Settings, on page 230.

IP Addressing and Routing

**Problem**
The IP addressing and routing fields may not be correctly configured.

**Solution**
You should verify the IP addressing and routing settings on the phone. If you are using DHCP, the DHCP server should provide these values. If you have assigned a static IP address to the phone, you must enter these values manually. See Check DHCP settings, on page 230.

DNS Settings

**Problem**
The DNS settings may be incorrect.
Solution
If you are using DNS to refer to the TFTP server or to Cisco Unified Communications Manager, you must ensure that you have specified a DNS server. See Verify DNS Settings, on page 231.

Cisco Unified Communications Manager Settings on Phone

Problem
The phone may have the wrong Cisco Unified Communications Manager information.

Solution
On the Cisco Unified IP Phone, press the Settings button, choose Device Configuration, and look at the Unified CM Configuration options. The Cisco Unified IP Phone attempts to open a TCP connection to all the Cisco Unified Communications Manager servers that are part of the assigned Cisco Unified Communications Manager group. If none of these options contain IP addresses or show Active or Standby, the phone is not properly registered with Cisco Unified Communications Manager. See Cisco Unified Communications Manager Phone Registration, on page 220 for tips on resolving this problem.

Cisco CallManager and TFTP Services Are Not Running

Problem
If the Cisco CallManager or TFTP services are not running, phones may not be able to start up properly. In such a situation, it is likely that you are experiencing a systemwide failure, and other phones and devices are unable to start up properly.

Solution
If the Cisco CallManager service is not running, all devices on the network that rely on it to make phone calls are affected. If the TFTP service is not running, many devices cannot start up successfully. For more information, see Start Service, on page 232.

Configuration File Corruption

Problem
If you continue to have problems with a particular phone that other suggestions in this chapter do not resolve, the configuration file may be corrupted.

Solution
Create a new phone configuration file. See Create New Phone Configuration File, on page 231.

Cisco Unified Communications Manager Phone Registration

Problem
The phone is not registered with Cisco Unified Communications Manager.
**Solution**

A Cisco Unified IP Phone can register with a Cisco Unified Communications Manager server only if the phone has been added to the server or if autoregistration is enabled. Review the information and procedures in *Cisco Unified Communications Manager Phone Addition Methods*, on page 37 to ensure that the phone has been added to the Cisco Unified Communications Manager database.

To verify that the phone is in the Cisco Unified Communications Manager database, choose **Device > Phone > Find** from Cisco Unified Communications Manager Administration to search for the phone based on the MAC Address. For information about determining a MAC address, see *Cisco Unified IP Phone MAC Address Determination*, on page 41.

If the phone is already in the Cisco Unified Communications Manager database, its configuration file may be damaged. See **Configuration File Corruption**, on page 220 for assistance.

**Cisco Unified IP Phone Cannot Obtain IP Address**

**Problem**

If a phone cannot obtain an IP address when it starts up, the phone may not be on the same network or VLAN as the DHCP server, or the switch port to which the phone connects may be disabled.

**Solution**

Ensure that the network or VLAN to which the phone connects has access to the DHCP server, and ensure that the switch port is enabled.

**Cisco Unified IP Phone Displays Security Error Message**

**Problem**

The phone displays “Security Error” on the screen.

**Cause**

When a Cisco Unified IP Phone boots, it performs an internal Power On Self Test (POST). POST checks for existing encryption functionality. If POST detects that encryption functionality is missing, the phone fails to boot, and the message “Security Error” appears on the screen.

**Solution**

To correct the problem, perform the following steps:

1. Reset the phone manually.
2. If the phone does not start up properly, power up the phone with the handset off-hook. When the phone is powered up in this way, it attempts to launch a backup software image.
3. If the phone still does not start up properly, perform a factory reset of the phone. For instructions, see **Factory Reset**, on page 237.
Cisco Unified IP Phone Resets Unexpectedly

If users report that their phones are resetting during calls or while idle on their desk, you should investigate the cause. If the network connection and Cisco Unified Communications Manager connection are stable, a Cisco Unified IP Phone should not reset on its own.

Typically, a phone resets if it has problems connecting to the Ethernet network or to Cisco Unified Communications Manager. These sections can help you identify the cause of a phone resetting in your network:

**Physical Connection Problems**

**Problem**
The physical connection to the LAN may be broken.

**Solution**
Verify that the Ethernet connection to which the Cisco Unified IP Phone connects is up. For example, check whether the particular port or switch to which the phone connects is down and that the switch is not rebooting. Also ensure that no cable breaks exist.

**Intermittent Network Outages**

**Problem**
Your network may be experiencing intermittent outages.

**Solution**
Intermittent network outages affect data and voice traffic differently. Your network might be experiencing intermittent outages without detection. If so, data traffic can resend lost packets and verify that packets are received and transmitted. However, voice traffic cannot recapture lost packets. Rather than retransmitting a lost network connection, the phone resets and attempts to reconnect to the network. Contact the system administrator for information on known problems in the voice network.

**DHCP Setting Errors**

**Problem**
The DHCP settings may be incorrect.

**Solution**
The following suggestions can help you determine if the phone has been properly configured to use DHCP:

1. Verify that you have properly configured the phone to use DHCP. For more information, see Network Configuration Menu, on page 66.
2. Verify that the DHCP server has been set up properly.
3. Verify the DHCP lease duration. Cisco recommends that you set it to 8 days. Cisco Unified IP Phone 7971G-GE and 7970G send messages with request type 151 to renew their DHCP address leases. If the DHCP server expects messages with request type 150, the lease will be denied, forcing the Cisco Unified IP Phone 7971G-GE and 7970G to restart and request a new IP address from the DHCP server.

**Static IP Address Setting Errors**

**Problem**
The static IP address assigned to the phone may be incorrect.

**Solution**
If the phone has been assigned a static IP address, verify that you have entered the correct settings.

**Voice VLAN Setup Errors**

**Problem**
If the Cisco Unified IP Phone appears to reset during heavy network usage (for example, following extensive web surfing on a computer connected to same switch as phone), it is likely that you do not have a voice VLAN configured.

**Solution**
Isolating the phones on a separate auxiliary VLAN increases the quality of the voice traffic.

**Phones Have Not Been Intentionally Reset**

**Problem**
If you are not the only administrator with access to Cisco Unified Communications Manager, you should verify that no one else has intentionally reset the phones.

**Solution**
You can check whether a Cisco Unified IP Phone received a command from Cisco Unified Communications Manager to reset by pressing the **Applications Menu** button on the phone and choosing **Settings > Status > Network Statistics**. If the phone was recently reset one of these messages appears:

- Reset-Reset: Phone received a Reset-Reset request from Cisco Unified Communications Manager Administration.
- Reset-Restart: Phone received a Reset-Restart request from Cisco Unified Communications Manager Administration.
DNS or Other Connectivity Errors

**Problem**
The phone reset continues and you suspect DNS or other connectivity issues.

**Solution**
If the phone continues to reset, eliminate DNS or other connectivity errors with Determine DNS or Connectivity Issues, on page 233.

Power Connection Problems

**Problem**
The phone does not appear to be powered up.

**Solution**
In most cases, a phone restarts if it powers up by using external power but loses that connection and switches to PoE. Similarly, a phone may restart if it powers up by using PoE and then connects to an external power supply.

Cisco Unified IP Phone Security Problems

The following sections provide troubleshooting information for the security features on the Cisco Unified IP Phone. For information about the solutions for any of these issues, and for additional troubleshooting information about security, see *Cisco Unified Communications Manager Security Guide*.

CTL File Problems

The following sections assist in troubleshooting CTL file problems.

**Authentication Error, Phone Cannot Authenticate CTL File**

**Problem**
A device authentication error occurs.

**Cause**
CTL file does not have a Cisco Unified Communications Manager certificate or has an incorrect certificate.

**Solution**
Install a correct certificate.
Phone Cannot Authenticate CTL File

Problem
Phone cannot authenticate the CTL file.

Cause
The security token that signed the updated CTL file does not exist in the CTL file on the phone.

Solution
Change the security token in the CTL file and install the new file on the phone.

ITL File Authenticates but Other Configuration Files Do Not Authenticate

Problem
Phone cannot authenticate any configuration files other than the ITL file.

Cause
The configuration file may not be signed by the corresponding certificate in the phone Trust List.

Solution
Re-sign the configuration file by using the correct certificate.

Phone Does Not Register

Problem
Phone does not register with Cisco Unified Communications Manager.

Cause
The CTL file does not contain the correct information for the Cisco Unified Communications Manager server.

Solution
Change the Cisco Unified Communications Manager server information in the CTL file.

Signed Configuration Files Are Not Requested

Problem
Phone does not request signed configuration files.

Cause
The CTL file does not contain any TFTP entries with certificates.
Solution
Configure TFTP entries with certificates in the CTL file.

802.1X Authentication Problems

802.1X authentication problems can be broken into the categories described in the following table.

Table 53: Identifying 802.1X Authentication Problems

<table>
<thead>
<tr>
<th>If all the following conditions apply,</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Phone cannot obtain a DHCP-assigned IP address.</td>
<td>802.1X Enabled on Phone but Phone Does Not Authenticate, on page 227</td>
</tr>
<tr>
<td>• Phone does not register with Cisco Unified Communications Manager.</td>
<td></td>
</tr>
<tr>
<td>• Phone status displays as “Configuring IP” or “Registering.”</td>
<td></td>
</tr>
<tr>
<td>• 802.1X Authentication Status displays as “Held” (see 802.1X Authentication and Status Menus, on page 116 for more details).</td>
<td></td>
</tr>
<tr>
<td>• Status menu displays 802.1X status as “Failed” (see Status Menu, on page 179 for more details).</td>
<td></td>
</tr>
<tr>
<td>• Phone cannot obtain a DHCP-assigned IP address</td>
<td>802.1X Not Enabled, on page 227</td>
</tr>
<tr>
<td>• Phone does not register with Cisco Unified Communications Manager</td>
<td></td>
</tr>
<tr>
<td>• Phone status display as “Configuring IP” or “Registering”</td>
<td></td>
</tr>
<tr>
<td>• 802.1X Authentication Status displays as “Disabled”</td>
<td></td>
</tr>
<tr>
<td>• Status menu displays DHCP status as timing out</td>
<td></td>
</tr>
</tbody>
</table>
If all the following conditions apply, See

- Phone cannot obtain a DHCP-assigned IP address.
- Phone does not register with Cisco Unified Communications Manager.
- Phone status display as “Configuring IP” or "Registering.”
- Cannot access phone menus to verify 802.1X status.

Factory Reset of Phone Has Deleted 802.1X Shared Secret, on page 228

802.1X Enabled on Phone but Phone Does Not Authenticate

Problem
The phone cannot authenticate.

Cause
These errors typically indicate that 802.1X authentication is enabled on the phone, but the phone is unable to authenticate.

1 Verify that you have properly configured the required components (see 802.1X Authentication, on page 21 for more information).

2 Confirm that the shared secret is configured on the phone (see 802.1X Authentication and Status Menus, on page 116 for more information).
   - If the shared secret is configured, verify that you have the same shared secret entered on the authentication server.
   - If the shared secret is not configured, enter it, and ensure that it matches the one on the authentication server.

802.1X Not Enabled

Problem
The phone does not have 802.1X configured.

Cause
These errors typically indicate that 802.1X authentication is not enabled on the phone.

Solution
To enable it, see 802.1X Authentication and Status Menus, on page 116.
Factory Reset of Phone Has Deleted 802.1X Shared Secret

**Problem**
After a reset, the phone does not authenticate.

**Cause**
These errors typically indicate that the phone has completed a factory reset (see Factory Reset, on page 237) while 802.1X was enabled. A factory reset deletes the shared secret, which is required for 802.1X authentication and network access.

**Solution**
To resolve this, you have two options:

- Temporarily disable 802.1X authentication on the switch.
- Temporarily move the phone to a network environment that is not using 802.1X authentication.

Once the phone starts up normally in one of these conditions, you can access the 802.1X configuration menus and re-enter the shared secret (see 802.1X Authentication and Status Menus, on page 116).

Audio and Video Problems

The following sections describe how to resolve audio and video problems.

**Phone Display Is Wavy**

**Problem**
The display appears to have rolling lines or a wavy pattern.

**Cause**
The phone might be interacting with certain types of older fluorescent lights in the building.

**Solution**
Move the phone away from the lights or replace the lights to resolve the problem.

**No Speech Path**

**Problem**
one or more people on a call do not hear any audio.
Solution
When at least one person in a call does not receive audio, IP connectivity between phones is not established. Check the configuration of routers and switches to ensure that IP connectivity is properly configured.

General Telephone Call Problems
This section describes troubleshooting of general telephone call problems.

VPN-Connected Phone Does Not Log Calls

Problem
A remote location (home office) phone that is connected through the VPN does not log missed, placed, or received calls.

Cause
Without explicitly setting the Alternate TFTP setting, the Cisco IP Phone cannot contact the TFTP server and download the configuration and other files, and function properly.

Solution
Set up the phone to use the Alternate TFTP server and configure the TFTP server IP address.

Related Topics
Set Up Remote Phone, on page 230

Phone Does Not Recognize DTMF Digits or Digits Are Delayed

Problem
The user complains that numbers are missed or delayed when the keypad is used.

Cause
Pressing the keys too quickly can result in missed or delayed digits.

Solution
Keys should not be pressed rapidly.

Troubleshooting Procedures
These procedures can be used to identify and correct problems.
Set Up Remote Phone

Cisco IP Phones that are configured for SSL VPN to ASA using the built-in client in a remote location (for example, a home office) have a special configuration requirement.

We recommend that you provide the phone with an Alternate TFTP server setting manually. This setting allows the phone to download the configuration and other files from TFTP. The phone in a remote location (home office) cannot correctly provide OPTION 150 to the phone using DHCP.

The IP phone can register to the last-known Cisco Unified Communications Manager, but any configuration updates cannot be applied until you configure the manual TFTP server address.

Procedure

Step 1 On the phone, select Applications.
Step 2 Navigate to the IPv4 Settings window.
Step 3 Scroll to the Alternate TFTP option and set the field to Yes.
Step 4 In the TFTP Server 1 field, set the TFTP server address.
Step 5 Save the changes.

Check TFTP Settings

Procedure

Step 1 You can determine the IP address of the TFTP server used by the phone by pressing the Settings button on the phone, choosing Network Configuration > IPv4, and scrolling to the TFTP Server 1 option.
Step 2 If you have assigned a static IP address to the phone, you must manually enter a setting for the TFTP Server 1 option. See Network Configuration Menu, on page 66.
Step 3 If you are using DHCP, the phone obtains the address for the TFTP server from the DHCP server. Check the IP address configured in Option 150.
Step 4 You can also enable the phone to use an alternate TFTP server. Such a setting is particularly useful if the phone was recently moved from one location to another. See Network Configuration Menu, on page 66 for instructions.

Check DHCP settings

Procedure

Step 1 On the Cisco Unified IP Phone, press the Settings button, choose Network Configuration, and look at the following options:
• DHCP Server: If you have assigned a static IP address to the phone, you do not need to enter a value for the DHCP Server option. However, if you are using a DHCP server, this option must have a value. If it does not, check your IP routing and VLAN configuration. See Troubleshooting Switch Port Problems at this URL: http://www.cisco.com/en/US/products/hw/switches/ps708/prod_tech_notes_list.html

• IP Address, Subnet Mask, Default Router: If you have assigned a static IP address to the phone, you must manually enter settings for these options. See Network Configuration Menu, on page 66 for instructions.

Step 2 If you are using DHCP, check the IP addresses distributed by your DHCP server. See Understanding and Troubleshooting DHCP in Catalyst Switch or Enterprise Networks at this URL: http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a00800f0804.shtml

Verify DNS Settings

To verify DNS settings, perform these steps.

Procedure

Step 1 Verify this setting by pressing Settings.
Step 2 Choose Network Configuration and scroll to the DNS Server 1 option.
Step 3 Verify that a CNAME entry exists in the DNS server for the TFTP server and for the Cisco Unified Communications Manager system.
Step 4 Ensure that DNS is configured to do reverse look-ups.

Create New Phone Configuration File

If you continue to have problems with a particular phone that other suggestions in this chapter do not resolve, the configuration file may be corrupted.
• When you remove a phone from the Cisco Unified Communications Manager database, the configuration file is deleted from the Cisco Unified Communications Manager TFTP server. The phone directory number or numbers remain in the Cisco Unified Communications Manager database. They are called “unassigned DNs” and can be used for other devices. If unassigned DNs are not used by other devices, delete them from the Cisco Unified Communications Manager database. You can use the Route Plan Report to view and delete unassigned reference numbers. See the Cisco Unified Communications Manager Administration Guide for more information.

• Changing the buttons on a phone button template, or assigning a different phone button template to a phone, may result in directory numbers that are no longer accessible from the phone. The directory numbers are still assigned to the phone in the Cisco Unified Communications Manager database, but the phone has no button with which calls can be answered. These directory numbers should be removed from the phone and deleted if necessary.

To create a new configuration file, follow these steps:

**Procedure**

**Step 1** From Cisco Unified Communications Manager, choose Device > Phone > Find to locate the phone experiencing problems.

**Step 2** Choose Delete to remove the phone from the Cisco Unified Communications Manager database.

**Step 3** Add the phone back to the Cisco Unified Communications Manager database. See Cisco Unified Communications Manager Phone Addition Methods, on page 37 for details.

**Step 4** Power cycle the phone.

**Start Service**

**Note** A service must be activated before it can be started or stopped. To activate a service, choose Tools > Service Activation.

To start a service, follow these steps:

**Procedure**

**Step 1** From Cisco Unified Communications Manager Administration, choose Cisco Unified Serviceability from the Navigation drop-down list and click Go.

**Step 2** Choose Tools > Control Center - Feature Services.

**Step 3** Choose the primary Cisco Unified Communications Manager server from the Server drop-down list. The window displays the service names for the server that you chose, the status of the services, and a service control panel to start or stop a service.

**Step 4** If a service has stopped, click the corresponding radio button and then click Start.
The Service Status symbol changes from a square to an arrow.

### Determine DNS or Connectivity Issues

If the phone continues to reset, follow these steps to eliminate DNS or other connectivity errors:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Use the <strong>Erase</strong> softkey to reset phone settings to their default values. See <em>Cisco Unified IP Phone Reset or Restore</em>, on page 236 for details.</td>
</tr>
</tbody>
</table>
| Step 2 | Modify DHCP and IP settings:  
  a) Disable DHCP. See *Network Configuration Menu*, on page 66 for instructions.  
  b) Assign static IP values to the phone. See *Network Configuration Menu*, on page 66 for instructions. Use the same default router setting used for other functioning Cisco Unified IP Phones.  
  c) Assign TFTP server. See *Network Configuration Menu*, on page 66 for instructions. Use the same TFTP server used for other functioning Cisco Unified IP Phones. |
| Step 3 | On the Cisco Unified Communications Manager server, verify that the local host files have the correct Cisco Unified Communications Manager server name mapped to the correct IP address. |
| Step 4 | From Cisco Unified Communications Manager, choose **System > Server** and verify that the server is referred to by the IP address and not by its DNS name. |
| Step 5 | From Cisco Unified Communications Manager, choose **Device > Phone** and verify that you have assigned the correct MAC address to this Cisco Unified IP Phone. For information about determining a MAC address, see *Cisco Unified IP Phone MAC Address Determination*, on page 41. |
| Step 6 | Power cycle the phone. |

### General Troubleshooting Information

The following table provides general troubleshooting information for the Cisco Unified IP Phone.

**Table 54: Cisco Unified IP Phone Troubleshooting**

<table>
<thead>
<tr>
<th>Summary</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Daisy-chaining IP phones</td>
<td>Cisco does not support connecting an IP phone to another IP phone through the PC port. Each IP phone should directly connect to a switch port. If phones are connected together in a line (by using the PC port), the phones do not work.</td>
</tr>
<tr>
<td>Poor quality when calling mobile phones using the G.729 protocol</td>
<td>In Cisco Unified Communications Manager, you can configure the network to use the G.729 protocol (the default is G.711). When using G.729, calls between an IP phone and a mobile phone will have poor voice quality. Use G.729 only when absolutely necessary.</td>
</tr>
<tr>
<td>Summary</td>
<td>Explanation</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>Prolonged broadcast storms cause IP phones to reset, or be unable to make or answer a call</td>
<td>A prolonged Layer 2 broadcast storm (lasting several minutes) on the voice VLAN may cause IP phones to reset, lose an active call, or be unable to initiate or answer a call. Phones may not come up until a broadcast storm ends.</td>
</tr>
<tr>
<td>Moving a network connection from the phone to a workstation</td>
<td>If you are powering your phone through the network connection, you must be careful if you decide to unplug the phone network connection and plug the cable into a desktop computer. <strong>Caution</strong> The computer network card cannot receive power through the network connection; if power comes through the connection, the network card can be destroyed. To protect a network card, wait 10 seconds or longer after unplugging the cable from the phone before plugging it into a computer. This delay gives the switch enough time to recognize that no phone is on the line and to stop providing power to the cable.</td>
</tr>
<tr>
<td>Changing the telephone configuration</td>
<td>By default, the network configuration options are locked to prevent users from making changes that could impact their network connectivity. You must unlock the network configuration options before you can configure them. See Unlock and Lock Options, on page 63 for details.</td>
</tr>
<tr>
<td>Codec mismatch between the phone and another device</td>
<td>The RxType and the TxType statistics show the codec that is used for a conversation between this Cisco Unified IP Phone and the other device. The values of these statistics should match. If they do not, verify that the other device can handle the codec conversation or that a transcoder is in place to handle the service. See Call Statistics Screen, on page 193 for information about displaying these statistics.</td>
</tr>
<tr>
<td>Sound sample mismatch between the phone and another device</td>
<td>The RxSize and the TxSize statistics show the size of the voice packets that are used in a conversation between this Cisco Unified IP phone and the other device. The values of these statistics should match. See Call Statistics Screen, on page 193 for information about displaying these statistics.</td>
</tr>
<tr>
<td>Gaps in voice calls</td>
<td>Check the AvgJtr and the MaxJtr statistics. A large variance between these statistics might indicate a problem with jitter on the network or periodic high rates of network activity. See Call Statistics Screen, on page 193 for information about displaying these statistics.</td>
</tr>
<tr>
<td><strong>Summary</strong></td>
<td><strong>Explanation</strong></td>
</tr>
<tr>
<td>----------------</td>
<td>----------------</td>
</tr>
</tbody>
</table>
| Loopback condition | A loopback condition can occur when the following conditions are met:  
  • The SW Port Configuration option in the Network Configuration menu on the phone is set to **10 Half** (10-BaseT/half duplex).  
  • The phone receives power from an external power supply.  
  • The phone is powered down (the power supply is disconnected).  
  
  In this case, the switch port on the phone can become disabled and the following message will appear in the switch console log:  
  `HALF_DUX_COLLISION_EXCEED_THRESHOLD`  
  To resolve this problem, re-enable the port from the switch. |
| Peer to peer image distribution fails. | If the peer to peer image distribution fails, the phone will default to using the TFTP server to download firmware. Access the log messages stored on the remote logging machine to help debug the peer to peer image distribution feature.  
  **Note**  
  These log messages are different than the log messages sent to the phone log. |
| Cisco VT Advantage/ Unified Video Advantage (CVTA) | If you are having problems getting CVTA to work, make sure that the PC Port is enabled, and that CDP is enabled on the PC port. |
| Phone call cannot be established | The phone does not have a DHCP IP address, is unable to register to Cisco Unified Communications Manager, and shows a Configuring IP or Registering message.  
  Verify the following:  
  1 The Ethernet cable is attached.  
  2 The Cisco CallManager service is running on the Cisco Unified Communications Manager server.  
  3 Both phones are registered to the same Cisco Unified Communications Manager.  
  4 Audio server debug and capture logs are enabled for both phones. If needed, enable Java debug. |
Summary | Explanation
--- | ---
Call established with the iLBC protocol does not show that the iLBC codec is being used | Call statistics display does not show iLBC as the receiver/sender codec.

1. Check the following by using Cisco Unified Communications Manager Administration:
   - Both phones are in the iLBC device pool.
   - The iLBC device pool is configured with the iLBC region.
   - The iLBC region is configured with the iLBC codec.

2. Capture a sniffer trace between the phone and Cisco Unified Communications Manager and verify that SCCP messages, OpenReceiveChannel, and StationMediaTransmit messages have media payload type value equal to 86. If so, the problem is with the phone; otherwise, the problem is with the Cisco Unified Communications Manager configuration.

3. Enable audio server debug and capture logs from both phones. If needed, enable Java debug.

**General Troubleshooting Tips for Cisco Unified IP Phone Expansion Module**

The following table provides general troubleshooting information for the Cisco Unified IP Phone Expansion Module.

*Table 55: Cisco Unified IP Phone Expansion Module Troubleshooting*

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>No display on the Cisco Unified IP Phone Expansion Module.</td>
<td>Verify that all of the cable connections are correct. Verify that you have power to the Cisco Unified IP Phone Expansion Module.</td>
</tr>
<tr>
<td>Lighted buttons on the first Cisco Unified IP Phone Expansion Module are all red.</td>
<td>Verify that the Cisco Unified IP Phone Expansion Module is configured in Cisco Unified Communications Manager.</td>
</tr>
<tr>
<td>Lighted buttons on the second Cisco Unified IP Phone Expansion Module are all amber.</td>
<td>Verify that the Cisco Unified IP Phone Expansion Module is configured in Cisco Unified Communications Manager.</td>
</tr>
</tbody>
</table>

**Cisco Unified IP Phone Reset or Restore**

Two methods exist for resetting or restoring the Cisco Unified IP Phone:
Basic Reset

Performing a basic reset of a Cisco Unified IP Phone provides a way to recover if the phone experiences an error and provides a way to reset or restore various configuration and security settings.

The following table describes the ways to perform a basic reset. You can reset a phone with any of these operations any time after the phone has started up. Choose the operation that is appropriate for your situation.

Table 56: Basic Reset Methods

<table>
<thead>
<tr>
<th>Operation</th>
<th>Performing</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restart phone</td>
<td>From the Main screen, press Settings to display the Settings menu, then press *<strong>#.</strong> Note: This factory reset sequence also works from any other screen that does not accept user input.</td>
<td>Resets any user and network configuration changes that you have made but that the phone has not written to the flash memory to previously saved settings, then restarts the phone.</td>
</tr>
<tr>
<td>Erase softkey</td>
<td>From the Settings menu, unlock phone options (see Unlock and Lock Options, on page 63). Then press Erase.</td>
<td>Resets user and network configuration settings to their default values, deletes the CTL file from the phone, and restarts the phone.</td>
</tr>
<tr>
<td></td>
<td>From the Network Configuration menu, unlock phone options (see Unlock and Lock Options, on page 63). Then press Erase.</td>
<td>Resets network configuration settings to their default values and resets the phone. (This method causes DHCP to reconfigure the IP address of the phone.)</td>
</tr>
<tr>
<td></td>
<td>From the Security Configuration menu, unlock phone options (see Unlock and Lock Options, on page 63). Then press the Erase softkey.</td>
<td>Deletes the CTL file from the phone and restarts the phone.</td>
</tr>
</tbody>
</table>

Factory Reset

When you perform a factory reset of the Cisco Unified IP Phone, the following information is erased or reset to its default value:

- CTL file: Erased
- LSC: Erased
- User configuration settings: Reset to default values
- Network configuration settings: Reset to default values
- Call histories: Erased
- Locale information: Reset to default values
• Phone application: Erased (phone recovers by loading the appropriate default load file, which depends on the phone model term75.default.loads, term71.default.loads, term70.default.loads, term65.default.loads, or term45.default.loads)

Before you perform a factory reset, ensure that the following conditions are met:

• The phone must be on a DHCP-enabled network.
• A valid TFTP server must be set in DHCP option 150 or option 66 on the DHCP server.
• The default load file for your phone model and the files specified in that file should be available on the TFTP server that is specified by the DHCP packet.

To perform a factory reset of a phone, follow these steps:

**Procedure**

**Step 1** Unplug the power cable from the phone and then plug it back in. The phone begins the power-up cycle.

**Step 2** While the phone is powering up, and before the Speaker button flashes on and off, press and hold #. Continue to hold # until each line button flashes on and off in sequence in orange (for the Cisco Unified IP Phone 7975G, 7971G-GE and 7970G) or amber (for the Cisco Unified IP Phone 7965G and 7945G).

**Step 3** Release # and press 123456789*0#. You can press a key twice in a row, but if you press the keys out of sequence, the factory reset does not take place.

After you press these keys, the line buttons on the phone flash orange and then green (for the Cisco Unified IP Phone 7975G, 7971G-GE and 7970G) or red (for the Cisco Unified IP Phone 7965G and 7945G), and the phone goes through the factory reset process. This process can take several minutes.

Do not power down the phone until it completes the factory reset process, and the main screen displays.

**Additional Troubleshooting Information**

If you have additional questions about troubleshooting the Cisco Unified IP Phones, these Cisco.com websites provide you with more tips.

• Cisco Unified IP Phone Troubleshooting Resources:
• Cisco Products and Services (Technical Support and Documentation):

**Maintenance**

This section contains the following topics
Quality Report Tool

The Quality Report Tool (QRT) is a voice quality and general problem-reporting tool for the Cisco Unified IP Phone. The QRT feature is installed as part of the Cisco Unified Communications Manager installation.

You can configure Cisco Unified IP Phones with QRT. When you do so, users can report problems with phone calls pressing QRT. This softkey is available only when the Cisco Unified IP Phone is in the Connected, Connected Conference, Connected Transfer, or OnHook states.

When a user presses QRT, a list of problem categories appears. The user selects the appropriate problem category, and this feedback is logged in an XML file. Actual information logged depends on the user selection, and if the destination device is a Cisco Unified IP Phone.

For more information about using QRT, see the Cisco Unified Serviceability Administration Guide.

Voice Quality Monitoring

To measure the voice quality of calls that are sent and received within the network, Cisco Unified IP Phones use these statistical metrics based on concealment events. The Digital Signal Processor (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.

- **MOS-LQK metrics:** Use a numeric score to estimate the relative voice listening quality. The Cisco Unified IP Phone calculates the mean opinion score (MOS) for listening quality (LQK) based audible concealment events due to frame loss in the preceding 8 seconds, and includes perceptual weighting factors such as codec type and frame size.

MOS LQK scores are produced by a Cisco proprietary algorithm, Cisco Voice Transmission Quality (CVTQ) index. Depending on the MOS LQK version number, these scores might be compliant with the International Telecommunications Union (ITU) standard P.564. This standard defines evaluation methods and performance accuracy targets that predict listening quality scores based on observation of actual network impairment.

Note

Concealment ratio and concealment seconds are primary measurements based on frame loss while MOS LQK scores project a "human-weighted" version of the same information on a scale from 5 (excellent) to 1 (bad) for measuring listening quality.

Listening quality scores (MOS LQK) relate to the clarity or sound of the received voice signal. Conversational quality scores (MOS CQ such as G.107) include impairment factors, such as delay, that degrade the natural flow of conversation.

You can access voice quality metrics from the Cisco Unified IP Phone by using the Call Statistics screen (see Call Statistics Screen, on page 193) or remotely by using Streaming Statistics (see Remote Monitoring, on page 199).
Voice Quality Metric Interpretation

To use the metrics for monitoring voice quality, note the typical scores under normal conditions of zero packet loss and use the metrics as a baseline for comparison.

It is important to distinguish significant changes from random changes in metrics. Significant changes are scores that change about 0.2 MOS or greater and persist in calls that last longer than 30 seconds. Conceal Ratio changes should indicate greater than 3 percent frame loss.

MOS LQK scores can vary based on the codec that the Cisco Unified IP Phone uses. The following codecs provide these maximum MOS LQK scores under normal conditions with zero frame loss:

• For Cisco Unified Phone 7975G, 7965G, and 7945G:
  ◦ G.711 gives 4.5 score.
  ◦ G.722 gives 4.5.
  ◦ G.728/iLBC gives 3.9.
  ◦ G.729A/AB gives 3.8.

• For Cisco Unified Phone 7971G-GE and 7970G:
  ◦ G.711 codec gives 4.5 score.
  ◦ G.729A/AB gives 3.7.

Note

• CVTQ does not support wideband (7 kHz) speech codecs, as ITU has not defined the extension of the technique to wideband. Therefore, MOS scores that correspond to G.711 performance are reported for G.722 calls to allow basic quality monitoring, rather than not reporting an MOS score.

• Reporting G.711-scale MOS scores for wideband calls through the use of CVTQ allows basic quality classifications to be indicated as good/normal or bad/abnormal. Calls with high scores (approximately 4.5) indicate high quality/low packet loss, and lower scores (approximately 3.5) indicate low quality/high packet loss.

• Unlike MOS, the Conceal Ratio and Concealed Seconds metrics remain valid and useful for both wideband and narrowband calls.

A Conceal Ratio of zero indicates that the IP network is delivering frames and packets on time with no loss.

Voice Quality Troubleshooting Tips

When you observe significant and persistent changes to metrics, use the following table for general troubleshooting information:
Table 57: Changes to Voice Quality Metrics

<table>
<thead>
<tr>
<th>Metric change</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>MOS LQK scores decrease significantly</td>
<td>Network impairment from packet loss or high jitter:</td>
</tr>
<tr>
<td></td>
<td>• Average MOS LQK decreases could indicate widespread and uniform impairment.</td>
</tr>
<tr>
<td></td>
<td>• Individual MOS LQK decreases indicate bursty impairment.</td>
</tr>
<tr>
<td></td>
<td>Cross-check with Conceal Ratio and Conceal Seconds for evidence of packet loss and jitter.</td>
</tr>
<tr>
<td>MOS LQK scores decrease significantly</td>
<td>Check to see whether the phone is using a different codec than expected (RxType and TxType).</td>
</tr>
<tr>
<td></td>
<td>Check to see whether the MOS LQK version changed after a firmware upgrade.</td>
</tr>
<tr>
<td>Conceal Ratio and Conceal Seconds</td>
<td>• Network impairment from packet loss or high jitter.</td>
</tr>
<tr>
<td>increase significantly</td>
<td></td>
</tr>
<tr>
<td>Conceal Ratio is near or at zero, but</td>
<td>Noise or distortion in the audio channel such as echo or audio levels.</td>
</tr>
<tr>
<td>the voice quality is poor.</td>
<td>Tandem calls that undergo multiple encode/decode, such as calls to a cellular network or calling card network.</td>
</tr>
<tr>
<td></td>
<td>Acoustic problems coming from a speakerphone, handsfree cellular phone, or wireless headset.</td>
</tr>
<tr>
<td></td>
<td>Check packet transmit (TxCnt) and packet receive (RxCnt) counters to verify that voice packets are flowing.</td>
</tr>
</tbody>
</table>

**Note**: Voice quality metrics do not account for noise or distortion, only frame loss.

---

**Cisco Unified IP Phone Cleaning**

To clean your Cisco Unified IP phone, use a soft, dry cloth to wipe the phone screen. Do not apply liquids or powders directly on the phone. As with all non-weather-proof electronics, liquids and powders can damage the components and cause failures.

Disable the screen before cleaning it so that you will not inadvertently choose a feature from the pressure of the cleaning cloth. To disable the screen, press **Display** for more than one second. The phone displays *Touchscreen Disabled* or *Phone Screen Disabled* and the **Display** button flashes green.

After one minute, the screen automatically reenables itself. To reenable the screen before that, press the flashing **Display** button for more than one second. The phone displays *Touchscreen Enabled* or *Phone Screen Enabled*.
Internal Support Web Site Overview

If you are a system administrator, you are likely the primary source of information for Cisco Unified IP Phone users in your network or company. It is important to provide current and thorough information to users. Cisco recommends that you create a web page on your internal support site that provides users with important information about their Cisco Unified IP Phones.

This chapter describes information that you might want on the support web site.

Cisco Unified IP Phone User Support

To successfully use some of the features on the Cisco Unified IP Phone (including Speed Dial, 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.
User Options Web Pages Access

Before a user can access the User Options web pages, you must use Cisco Unified Communications Manager Administration to add the user to a standard Cisco Unified Communications Manager End User group: choose User Management > User Groups. For more information, see:

- Cisco Unified Communications Manager Administration Guide, "User Group Configuration" chapter
- Cisco Unified Communications Manager System Guide, "Roles and User Groups" chapter

Online Help on Phone

The Cisco Unified IP Phones provide access to a comprehensive online help system. To view the main help menu on a phone, press the ? button. If you are already in Help, press Main.

Main menu topics include:

- About Your Cisco Unified IP Phone: Descriptive information about the phone model
- How do I...?: Procedures and information about commonly used phone tasks
- Calling Features: Descriptions and procedures for using calling features, such as conference and transfer
- Help: Tips on using and accessing Help

You can also use the ? button to obtain information about softkeys, menu items, and the help system itself. See your User Guide for more information.

Cisco Unified IP Phone Manuals

You should provide users with access to user documentation for the Cisco Unified IP Phones. Each user guide includes detailed user instructions for key phone features.

Several Cisco Unified IP Phone models are available, so to assist users in finding the appropriate documentation on the Cisco website, Cisco recommends that you provide links to the current documentation. If you do not want to or cannot send users to the Cisco website, Cisco suggests that you download the PDF files and provide them to the users on your website.

For a list of available documentation for Cisco Unified IP Phones, go to this URL:

For a list of available documentation for Cisco Unified Communications Manager, go to this URL:
Cisco Unified IP Phone 7900 Series eLearning Tutorials for SCCP Phones

Cisco Unified IP Phone 7900 Series eLearning tutorials use audio and animation to demonstrate basic calling features for SCCP phones. The eLearning tutorials are currently available for the Cisco Unified IP Phone 7970 Series (7970G, 7971G-GE) and the Cisco Unified IP Phone models 7905G, 7912G, 7940G, 7941G, 7941G-GE, 7960G, 7961G, and 7961G-GE.

Users can access runtime versions of the eLearning tutorials (English only) from Cisco.com by looking for tutorials under relevant phone models at this site:


Administrators can download customizable versions of the eLearning tutorials (English only) from the phone product pages on cisco.com at


Refer to the tutorial Read Me file that is included with the relevant eLearning tutorial for specific instructions, including how to link to the most recent user guide PDF.

---

**Note**

The eLearning tutorials are updated periodically and therefore might not contain the latest feature information for users. For the latest feature information, see the *Cisco Unified IP Phone User Guide* that applies to the phone model and Cisco Unified Communications Manager version.

---

Phone Features User Subscription and Setup

Users can perform a variety of activities by using the Cisco Unified Communications Manager User Options web pages. These activities include subscribing to services, setting up speed dial and call forwarding numbers, configuring ring settings, and creating a personal address book. Keep in mind that configuring settings on a phone using a website might be new for your users. You need to provide as much information as possible to ensure that they can successfully access and use the User Options web pages.

Make sure to provide users with the following information about the User Options web pages:

- The URL required to access the application. This URL is:

  http://<server_name:portnumber>/ccmuser/, where *server_name* is the host on which the web server is installed.

- A user ID and default password are needed to access the application.

  These settings correspond to the values you entered when you added the user to Cisco Unified Communications Manager (see *Cisco Unified Communications Manager User Addition*, on page 156).

- A brief description of what a web-based, graphical user interface application is, and how to access it with a web browser.

- An overview of the tasks that users can accomplish by using the web page.
User Voice Messaging System Access

Cisco Unified Communications Manager lets you integrate with different voice messaging systems, including the Cisco Unity voice messaging system. Because you can integrate with a variety of systems, you must provide users with information about how to use your specific system.

You should provide this information to each user:

- How to access the voice messaging system account.
  Make sure that you have used Cisco Unified Communications Manager to configure the Messages button on the Cisco Unified IP Phone.

- Initial password for accessing the voice messaging system.
  Make sure that you have configured a default voice messaging system password for all users.

- How the phone indicates that voice messages are waiting.
  Make sure that you have used Cisco Unified Communications Manager to set up a message waiting indicator (MWI) method.

User Personal Directory Entries Setup

Users can configure personal directory entries on the Cisco Unified IP Phone. To configure a personal directory, users must have access to the following:

- User Options web pages: Make sure that users know how to access their User Options web pages. See Phone Features User Subscription and Setup, on page 245 for details.

- Cisco Unified IP Phone Address Book Synchronizer: Make sure to provide users with the installer for this application:

Obtain Cisco Unified IP Phone Address Book Synchronizer

To download a copy of the synchronizer to send to your users, follow these steps:

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>To obtain the installer, choose Application &gt; Plugins from Cisco Unified Communications Manager Administration.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Select Download, which is located next to the Cisco Unified IP Phone Address Book Synchronizer plugin name.</td>
</tr>
<tr>
<td>Step 3</td>
<td>When the file download dialog box displays, select Save.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Send the TabSyncInstall.exe file and the instructions in Cisco Unified IP Phone Address Book Synchronizer Deployment, on page 247 to all users who require this application.</td>
</tr>
</tbody>
</table>
Cisco Unified IP Phone Address Book Synchronizer Deployment

The Cisco Unified IP Phone Address Book Synchronizer synchronizes data that is stored in your Microsoft Windows address book with the Cisco Unified Communications Manager directory and the User Options Personal Address Book.

Tip
To successfully synchronize the Windows address book with the Personal Address Book, all Windows address book users should be entered in the Windows address book before you perform the following procedures.

Install Synchronizer

To install the Cisco Unified IP Phone Address Book Synchronizer, follow these steps:

Procedure

Step 1
Get the Cisco Unified IP Phone Address Book Synchronizer installer file from your system administrator.

Step 2
Double-click the TabSyncInstall.exe file that your administrator provided. The publisher dialog box displays.

Step 3
Select Run.
The Welcome to the InstallShield Wizard for Cisco Unified CallManager Personal Address Book Synchronizer window displays.

Step 4
Select Next.
The License Agreement window displays.

Step 5
Read the license agreement information, and select the I Accept. Select Next.
The Destination Location window displays.

Step 6
Choose the directory in which you want to install the application and select Next.
The Ready to Install window displays.

Step 7
Select Install.
The installation wizard installs the application to your computer. When the installation is complete, the InstallShield Wizard Complete window displays.

Step 8
Select Finish.

Step 9
To complete the process, follow the steps in Set Up Synchronizer, on page 247.

Set Up Synchronizer

To configure the Cisco Unified IP Phone Address Book Synchronizer, perform these steps:
Procedure

Step 1  Open the Cisco Unified IP Phone Address Book Synchronizer.
If you accepted the default installation directory, you can open the application by choosing **Start > All Programs > Cisco Systems > TabSync**.

Step 2  To configure user information, select **User**.
The Cisco Unified CallManager User Information window displays.

Step 3  Enter the Cisco Unified IP Phone user name and password and select **OK**.

Step 4  To configure Cisco Unified Communications Manager server information, select **Server**.
The Configure Cisco Unified CallManager Server Information window displays.

Step 5  Enter the IP address or host name and the port number of the Cisco Unified Communications Manager server and select **OK**.
If you do not have this information, contact your system administrator.

Step 6  To start the directory synchronization process, select **Synchronize**.
The Synchronization Status window provides the status of the address book synchronization. If you chose the user intervention for duplicate entries rule and you have duplicate address book entries, the Duplicate Selection window displays.

Step 7  Choose the entry that you want to include in your Personal Address Book and select **OK**.

Step 8  When synchronization is complete, select **Exit** to close the Cisco Unified CallManager Address Book Synchronizer.

Step 9  To verify whether the synchronization worked, sign in to your User Options web pages and choose **Personal Address Book**. The users from your Windows address book should be listed.
# Feature Support by Protocol for Cisco Unified IP Phones

This appendix provides information about feature support for the Cisco Unified IP Phones using the SCCP or SIP protocol with Cisco Unified Communications Manager Release 8.6.

The following table provides a high-level overview of calling features and their support by protocol. This table focuses primarily on end user calling features and is not intended to represent a comprehensive listing of all available phone features. For details about user interface differences and feature use, see the *Cisco Unified IP Phone 7975G, 7971G-GE, 7970G, 7965G, and 7945G User Guide*.  
The guide is available at this URL:  
The specific sections that describe the features in the user guide are referenced in the table.

**Table 58: Cisco Unified IP Phone 7975G, 7971G-GE, 7970G, 7965G, and 7945G Feature Support by Protocol**

<table>
<thead>
<tr>
<th>Features</th>
<th>Protocol: SCCP</th>
<th>Protocol: SIP</th>
<th>For more information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Calling features</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Abbreviated Dialing</td>
<td>Supported</td>
<td>Supported</td>
<td>Calling features: Additional call options</td>
</tr>
<tr>
<td>Agent Greeting</td>
<td>Supported</td>
<td>Supported</td>
<td>Calling features: Call answer</td>
</tr>
<tr>
<td>Anonymous Call Block</td>
<td>Not supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Assisted Directed Call Park</td>
<td>Not supported</td>
<td>Supported</td>
<td>Calling features: Advanced call handling - Call park</td>
</tr>
<tr>
<td>Audible Message Waiting Indicator</td>
<td>Supported</td>
<td>Supported</td>
<td>Voice messages</td>
</tr>
<tr>
<td>AutoAnswer</td>
<td>Supported</td>
<td>Supported</td>
<td>Handset, headset, and speakerphone</td>
</tr>
<tr>
<td>Features</td>
<td>Protocol: SCCP</td>
<td>Protocol: SIP</td>
<td>For more information</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>----------------</td>
<td>---------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>Auto Call Pickup</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Auto Dial</td>
<td>Supported</td>
<td>Supported</td>
<td>Calling features: Basic call options</td>
</tr>
<tr>
<td>Barge (and cBarge)</td>
<td>Supported</td>
<td>Supported</td>
<td>Calling features: Advanced call handling - Shared lines</td>
</tr>
<tr>
<td>Block External to External Transfer</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Busy Lamp Field (BLF)</td>
<td>Supported</td>
<td>Supported</td>
<td>Calling features: Advanced call handling - Busy Lamp Field features</td>
</tr>
<tr>
<td>Busy Lamp Field (BLF) Pickup</td>
<td>Supported</td>
<td>Supported</td>
<td>Calling features: Advanced call handling - Busy Lamp Field features</td>
</tr>
<tr>
<td>Call Back</td>
<td>Supported</td>
<td>Supported</td>
<td>Calling features: Additional call options</td>
</tr>
<tr>
<td>Call Chaperone</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Call Display Restrictions</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Call Forward All</td>
<td>Supported</td>
<td>Supported</td>
<td>Calling features: Call Forward</td>
</tr>
<tr>
<td>Call Forward All Breakout</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Call Forward All Loop Prevention</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Call Forward Busy</td>
<td>Supported</td>
<td>Supported</td>
<td>Calling features: Call Forward</td>
</tr>
<tr>
<td>Call Forward Configurable Display</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Call Forward Destination Override</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Call Forward No Answer</td>
<td>Supported</td>
<td>Supported</td>
<td>Calling features: Call Forward</td>
</tr>
<tr>
<td>Call Park</td>
<td>Supported</td>
<td>Supported</td>
<td>Calling features: Advanced call handling - Call Park</td>
</tr>
<tr>
<td>Features</td>
<td>Protocol: SCCP</td>
<td>Protocol: SIP</td>
<td>For more information</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>----------------</td>
<td>---------------</td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Call Pickup</td>
<td>Supported</td>
<td>Supported</td>
<td>Calling features: Advanced call handling - Call PickUp</td>
</tr>
<tr>
<td>Group Call Pickup</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Directed Call Pickup</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other Call Pickup</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Call Recording</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Call Waiting</td>
<td>Supported</td>
<td>Supported</td>
<td>Calling features: Call answer</td>
</tr>
<tr>
<td>Caller ID</td>
<td>Supported</td>
<td>Supported</td>
<td>Phone features: Phone screen features</td>
</tr>
<tr>
<td>Caller ID Blocking</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Call Back</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Cisco Unified Communications Manager Assistant</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Cisco Extension Mobility</td>
<td>Supported</td>
<td>Supported</td>
<td>Calling features: Advanced call handling - Cisco Extension Mobility</td>
</tr>
<tr>
<td>Cisco Extension Mobility Change PIN</td>
<td>Supported</td>
<td>Supported</td>
<td>Calling features: Advanced call handling - Cisco Extension Mobility</td>
</tr>
<tr>
<td>Cisco Extension Mobility Cross Cluster</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Client Matter Codes (CMC)</td>
<td>Supported</td>
<td>Not supported</td>
<td>Calling features: Advanced call handling - Place call using billing or tracking code</td>
</tr>
<tr>
<td>Computer Telephony Integration (CTI) Applications</td>
<td>Supported</td>
<td>Some support (such as Call Park, MWI)</td>
<td></td>
</tr>
<tr>
<td>Configurable Call Forward Display</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Device Invoked Recording</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Direct Transfer</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Features</td>
<td>Protocol: SCCP</td>
<td>Protocol: SIP</td>
<td>For more information</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>----------------</td>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Directed Call Park</td>
<td>Supported</td>
<td>Supported</td>
<td>Calling features: Advanced call handling - Call Park</td>
</tr>
<tr>
<td>Do Not Disturb (DND)</td>
<td>Supported</td>
<td>Supported</td>
<td>Calling features: Do Not Disturb</td>
</tr>
<tr>
<td>Enbloc Dialing</td>
<td>Supported</td>
<td>Not Supported</td>
<td></td>
</tr>
<tr>
<td>Distinctive Ring</td>
<td>Supported</td>
<td>Supported</td>
<td>Phone customization: Rings and message indicator customization</td>
</tr>
<tr>
<td>Fast Dial Service</td>
<td>Supported</td>
<td>Supported</td>
<td>Calling features: Advanced call handling - Speed Dial</td>
</tr>
<tr>
<td>Forced Authorization Codes (FAC)</td>
<td>Supported</td>
<td>Not supported</td>
<td>Calling features: Additional call options - Place call using billing or tracking code</td>
</tr>
<tr>
<td>Group Call Pickup</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Headset Sidetone Control and Send Gain</td>
<td>Supported</td>
<td>Supported</td>
<td>Handset, headset, and speakerphone: Headset - Control wired headset sidetone and send gain</td>
</tr>
<tr>
<td>Headset Recording</td>
<td>Supported (7945G, 7965G, and 7975G only)</td>
<td>Supported (7945G, 7965G, and 7975G only)</td>
<td></td>
</tr>
<tr>
<td>Help System</td>
<td>Supported</td>
<td>Supported</td>
<td>Phone features: Feature buttons and menus</td>
</tr>
<tr>
<td>Hold/Resume</td>
<td>Supported</td>
<td>Supported</td>
<td>Calling features: Hold and resume</td>
</tr>
<tr>
<td>Hold Reversion</td>
<td>Supported</td>
<td>Supported</td>
<td>Calling features: Hold and resume</td>
</tr>
<tr>
<td>Hunt Group Display</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Immediate Divert</td>
<td>Supported</td>
<td>Supported</td>
<td>Calling features: Call answer</td>
</tr>
<tr>
<td>Immediate Divert—Enhanced</td>
<td>Supported</td>
<td>Supported</td>
<td>Calling features: Call transfer to voice message system</td>
</tr>
<tr>
<td>Intelligent Session Control</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Inter-Cluster Trust (Bulk Certificate Replication)</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Intercom</td>
<td>Supported</td>
<td>Supported</td>
<td>Calling features: Intercom calls</td>
</tr>
<tr>
<td>Features</td>
<td>Protocol: SCCP</td>
<td>Protocol: SIP</td>
<td>For more information</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>----------------</td>
<td>---------------</td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Intra-Cluster Trust (Bulk Certificate Replication)</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Join/Select</td>
<td>Supported</td>
<td>Supported</td>
<td>Calling features: Conference calls</td>
</tr>
<tr>
<td>Join Across Lines/Select</td>
<td>Supported</td>
<td>Supported</td>
<td>Calling features: Conference calls</td>
</tr>
<tr>
<td>Log Out of Hunt Groups</td>
<td>Supported</td>
<td>Supported</td>
<td>Calling features: Advanced call handling - Hunt Groups</td>
</tr>
<tr>
<td>Malicious Call ID</td>
<td>Supported</td>
<td>Supported</td>
<td>Calling features: Advanced call handling - Suspicious call trace</td>
</tr>
<tr>
<td>Meet-Me Conference</td>
<td>Supported</td>
<td>Supported</td>
<td>Calling features: Conference calls</td>
</tr>
<tr>
<td>Message Waiting Indicator</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Mobile Connect</td>
<td>Supported</td>
<td>Supported</td>
<td>Calling features: Advanced call handling - Cisco Extension Mobility</td>
</tr>
<tr>
<td>Mobile Voice Access</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Multilevel Precedence and Preemption (MLPP)</td>
<td>Supported</td>
<td>Not supported</td>
<td>Calling features: Advanced call handling - Priority calls</td>
</tr>
<tr>
<td>Multiple Calls per Line Appearance</td>
<td>200</td>
<td>50</td>
<td>Phone features: Line and call definitions</td>
</tr>
<tr>
<td>Music-on-Hold</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Mute</td>
<td>Supported</td>
<td>Supported</td>
<td>Calling features: Mute</td>
</tr>
<tr>
<td>Ringer Volume Control</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>On-hook Dialing/Pre-Dial</td>
<td>Supported</td>
<td>Supported</td>
<td>Calling features: Basic call options</td>
</tr>
<tr>
<td>Onhook Call Transfer</td>
<td>Supported</td>
<td>Supported</td>
<td>Calling features: Call transfer</td>
</tr>
<tr>
<td>Features</td>
<td>Protocol: SCCP</td>
<td>Protocol: SIP</td>
<td>For more information</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>----------------</td>
<td>---------------</td>
<td>------------------------------------------------------------</td>
</tr>
<tr>
<td>Other Group Pickup</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Plus Dialing</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Presence-Enabled Directories</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Privacy</td>
<td>Supported</td>
<td>Supported</td>
<td>Calling features: Advanced call handling - Shared lines</td>
</tr>
<tr>
<td>Private Line Automated Ringdown (PLAR)</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Programmable Line Keys</td>
<td>Supported</td>
<td>Supported</td>
<td>Calling features</td>
</tr>
<tr>
<td>Protected Calling</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Quality Reporting Tool (QRT)</td>
<td>Supported</td>
<td>Supported</td>
<td>Troubleshooting: Quality Reporting Tool</td>
</tr>
<tr>
<td>Redial</td>
<td>Supported</td>
<td>Supported</td>
<td>Calling features: Basic call options - Redial number</td>
</tr>
<tr>
<td>Ring Setting</td>
<td>Supported</td>
<td>Supported</td>
<td>Phone features: Buttons and hardware identification</td>
</tr>
<tr>
<td>Secure and Nonsecure Indication Tone</td>
<td>Supported</td>
<td>Supported</td>
<td>Calling features: Advanced call handling - Secure calls</td>
</tr>
<tr>
<td>Secure Conference</td>
<td>Supported</td>
<td>Supported</td>
<td>Calling features: Conference calls</td>
</tr>
<tr>
<td>Services</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Services URL button</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Session Handoff</td>
<td>Supported</td>
<td>Supported</td>
<td>Calling features: Call transfer</td>
</tr>
<tr>
<td>Shared Line</td>
<td>Supported</td>
<td>Supported</td>
<td>Calling features: Advanced call handling - Shared lines</td>
</tr>
<tr>
<td>Sidetone Level</td>
<td>Supported</td>
<td>Supported</td>
<td>Handset, headset, and speakerphone: Headset - Control</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>wired headset sidetone</td>
</tr>
<tr>
<td>Silent Monitoring</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Features</td>
<td>Protocol: SCCP</td>
<td>Protocol: SIP</td>
<td>For more information</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>----------------</td>
<td>---------------</td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Single Button Barge</td>
<td>Supported</td>
<td>Supported</td>
<td>Calling features: Advanced call handling - Shared lines - Barge, cBarge, and shared lines</td>
</tr>
<tr>
<td>Speed Dialing</td>
<td>Supported</td>
<td>Supported</td>
<td>Calling features: Advanced call handling - Speed Dial</td>
</tr>
<tr>
<td>SSH Access</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Time-of-Day Routing</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Touchscreen Illumination Disabling</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Transfer</td>
<td>Supported</td>
<td>Supported</td>
<td>Calling features: Call transfer</td>
</tr>
<tr>
<td>Transfer - Direct Transfer</td>
<td>Supported</td>
<td>Supported</td>
<td>Calling features: Call transfer</td>
</tr>
<tr>
<td>Time Zone Update</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>URL Dialing</td>
<td>Not supported</td>
<td>Supported</td>
<td>Call logs and directories: Call logs - Place call from URL entry in call log</td>
</tr>
<tr>
<td>Video Mode</td>
<td>Supported</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td>Video Support</td>
<td>Supported</td>
<td>Not supported</td>
<td>Additional options</td>
</tr>
<tr>
<td>Virtual Private Network Support in Phones</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Voice Mail</td>
<td>Supported</td>
<td>Supported</td>
<td>Voice messages</td>
</tr>
<tr>
<td>VPN Client</td>
<td>Supported (7945G, 7965G, and 7975G only)</td>
<td>Not supported</td>
<td>Calling features: Advanced call handling - Secure calls</td>
</tr>
<tr>
<td>WebDialer</td>
<td>Supported</td>
<td>Supported</td>
<td>User Options web pages: Features and services setup on web - Cisco WebDialer</td>
</tr>
</tbody>
</table>

**Settings**

<table>
<thead>
<tr>
<th>Automatic Port Synchronization</th>
<th>Supported</th>
<th>Supported</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Statistics</td>
<td>Supported</td>
<td>Supported</td>
<td>Troubleshooting: Phone troubleshooting data</td>
</tr>
<tr>
<td>Features</td>
<td>Protocol: SCCP</td>
<td>Protocol: SIP</td>
<td>For more information</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>----------------</td>
<td>---------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>Power Save Plus (EnergyWise)</td>
<td>Supported</td>
<td>Not supported</td>
<td>Phone features: Energy savings</td>
</tr>
<tr>
<td>Remote Port Configuration</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>SSH Disable</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>UCR 2008</td>
<td>Supported</td>
<td>Not Supported</td>
<td></td>
</tr>
<tr>
<td>Voice Quality Metrics</td>
<td>Supported</td>
<td>Supported</td>
<td>Troubleshooting: Phone troubleshooting data</td>
</tr>
</tbody>
</table>

**Services**

<table>
<thead>
<tr>
<th>Services</th>
<th>Protocol: SCCP</th>
<th>Protocol: SIP</th>
<th>For more information</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDK Compliance</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
</tbody>
</table>

**Directories**

<table>
<thead>
<tr>
<th>Directories</th>
<th>Protocol: SCCP</th>
<th>Protocol: SIP</th>
<th>For more information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Logs</td>
<td>Supported</td>
<td>Supported</td>
<td>Call logs and directories: Directory features</td>
</tr>
<tr>
<td>Corporate Directories</td>
<td>Supported</td>
<td>Supported</td>
<td>Call logs and directories: Directory features</td>
</tr>
<tr>
<td>Personal Directory Enhancements</td>
<td>Supported</td>
<td>Supported</td>
<td>Call logs and directories: Directory features</td>
</tr>
</tbody>
</table>

**Supplemental Features and Applications**

<table>
<thead>
<tr>
<th>Supplemental Features and Applications</th>
<th>Protocol: SCCP</th>
<th>Protocol: SIP</th>
<th>For more information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Communications Manager Assistant</td>
<td>Supported</td>
<td>Supported</td>
<td>Cisco Unified Communications Manager Assistant User Guide</td>
</tr>
<tr>
<td>Cisco Unified Communications Manager Auto-Attendant</td>
<td>Supported</td>
<td>Supported</td>
<td>Cisco Unified Communications Manager Features and Services Guide</td>
</tr>
<tr>
<td>Cisco Unified Business Attendant Console</td>
<td>Supported</td>
<td>Supported</td>
<td>These are third-party products. See Cisco Unified Attendant Consoles, Maintain and Operate Guides</td>
</tr>
<tr>
<td>Features</td>
<td>Protocol: SCCP</td>
<td>Protocol: SIP</td>
<td>For more information</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------------------------------------</td>
<td>------------------------------------</td>
<td>-----------------------------------------------------------</td>
</tr>
<tr>
<td>Cisco Unified IP Phone Expansion Module 7914</td>
<td>Supported (7965, 7970, 7971, 7975 only)</td>
<td>Supported (7965, 7970, 7971, 7975 only)</td>
<td>Cisco Unified IP Phone Expansion Module 7914 Guide</td>
</tr>
<tr>
<td>Cisco Unified IP Phone Expansion Module 7915</td>
<td>Supported (7965, 7975 only)</td>
<td>Supported (7965, 7975 only)</td>
<td>Cisco Unified IP Phone Expansion Module 7915 Guide</td>
</tr>
<tr>
<td>Cisco Unified IP Phone Expansion Module 7916</td>
<td>Supported (7965, 7975 only)</td>
<td>Supported (7965, 7975 only)</td>
<td>Cisco Unified IP Phone Expansion Module 7916 Guide</td>
</tr>
<tr>
<td>Cisco VT Advantage</td>
<td>Supported</td>
<td>Not supported</td>
<td>Cisco VT Advantage User Guide</td>
</tr>
</tbody>
</table>
International User Support

• International User Support Overview, page 259
• Language Overlays for Phone Buttons, page 259
• Unified Communications Manager Endpoints Locale Installer, page 259
• Language Limitation, page 260
• International Call Logging Support, page 260

International User Support Overview

Translated and localized versions of the Cisco Unified IP Phones are available in several languages. If you are supporting Cisco Unified IP Phones in a non-English environment, the following sections ensure that the phones are set up properly for your users.

Language Overlays for Phone Buttons

To support the needs of international users, the button labels on the Cisco Unified IP Phones display icons rather than text to indicate the purposes of the buttons. You can purchase language-specific text overlays to add to a phone. To order these language-specific overlays, go to this website:

http://www.overlaypro.com/cisco/

Phone overlays are available only for languages in which the Cisco Unified IP Phone software has been localized. All languages may not be available immediately, so continue to check the website for updates.

Unified Communications Manager Endpoints Locale Installer

By default, Cisco IP Phones are set up for the English (United States) locale. To use the Cisco IP Phones in other locales, you must install the locale-specific version of the Unified Communications Manager Endpoints Locale Installer on every Cisco Unified Communications Manager server in the cluster. The Locale Installer installs the latest translated text for the phone user interface and country-specific phone tones on your system so that they are available for the Cisco IP Phones.
To access the Locale Installer required for a release, access https://software.cisco.com/download/navigator.html?mdfid=286037605&flowid=46245, navigate to your phone model, and select the Unified Communications Manager Endpoints Locale Installer link.

For more information, see the documentation for your particular Cisco Unified Communications Manager release.

---

**Note**

The latest Locale Installer may not be immediately available; continue to check the website for updates.

---

**Language Limitation**

There is no localized Keyboard Alphanumeric Text Entry (KATE) support for the following Asian locales:

- Chinese (China)
- Chinese (Hong Kong)
- Chinese (Taiwan)
- Japanese (Japan)
- Korean (Korea Republic)

The default English (United States) KATE is presented to the user instead.

For example, the phone screen will show text in Korean, but the 2 key on the keypad will display a b c 2 A B C.

---

**International Call Logging Support**

If your phone system is configured for international call logging (calling party normalization), the call logs, redial, or call directory entries may display a plus (+) symbol to represent the international escape code for your location. Depending on the configuration for your phone system, the + may be replaced with the correct international dialing code, or you may need to edit the number before dialing to manually replace the + with the international escape code for your location. In addition, while the call log or directory entry may display the full international number for the received call, the phone display may show the shortened local version of the number, without international or country codes.
Technical Specifications

• Physical and Operating Environment Specifications, page 261
• Cable Specifications, page 263
• Network and Access Port Pinouts, page 263
• Phone Behavior During Times of Network Congestion, page 264

Physical and Operating Environment Specifications

The following table shows the physical and operating environment specifications for the Cisco Unified IP Phone.

**Table 59: Physical and Operating Specifications**

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value or range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating temperature</td>
<td>32° to 104°F (0° to 40°C)</td>
</tr>
<tr>
<td>Operating relative humidity</td>
<td>10% to 95% (non-condensing)</td>
</tr>
<tr>
<td>Storage temperature</td>
<td>14° to 140°F (~10° to 60°C)</td>
</tr>
<tr>
<td>Height</td>
<td>9.07 in. (23.03 cm)</td>
</tr>
<tr>
<td></td>
<td><strong>For Cisco Unified IP Phone 7975G:</strong></td>
</tr>
<tr>
<td></td>
<td>8.2 in. (20.32 cm)</td>
</tr>
<tr>
<td>Width</td>
<td><strong>For Cisco Unified IP Phone 7965G, and 7945G:</strong></td>
</tr>
<tr>
<td></td>
<td>10.82 in. (27.48 cm)</td>
</tr>
<tr>
<td></td>
<td><strong>For Cisco Unified IP Phone 7975G, 7971G-GE and 7970G:</strong></td>
</tr>
<tr>
<td></td>
<td>10.5 in. (26.67 cm)</td>
</tr>
<tr>
<td>Specification</td>
<td>Value or range</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Depth</td>
<td>• 2.54 in. (6.45 cm)—with footstand fully closed</td>
</tr>
<tr>
<td></td>
<td>• 6.0 in. (15.24 cm)—with footstand fully open</td>
</tr>
<tr>
<td></td>
<td>• 3.54 in. (9.00 cm)—with optional wall mount kit (Cisco Unified IP Phone 7975G, 7965G, and 7945G)</td>
</tr>
<tr>
<td>Weight</td>
<td>3.25 lb (1.47 kg)</td>
</tr>
<tr>
<td>Power options</td>
<td><strong>Cisco Unified IP Phone 7975G, 7965G and 7945G:</strong></td>
</tr>
<tr>
<td></td>
<td>• 100-240 VAC, 50-60 Hz, 0.5 A—when using the AC adapter</td>
</tr>
<tr>
<td></td>
<td>• 44V - 57V DC, 0.25 A—when using the in-line power over the network cable</td>
</tr>
<tr>
<td></td>
<td><strong>Cisco Unified IP Phone 7971G-GE and 7970G:</strong></td>
</tr>
<tr>
<td></td>
<td>• The phone can receive power from IEEE 802.3af-compliant data switches (Class III).</td>
</tr>
<tr>
<td></td>
<td>• The phone can be powered locally with a power adapter (Cisco part number CP-PWR-CUBE-3=) and the appropriate power cord (power requirements for the power adapter: 100-240 VAC, 50-60 Hz, 0.5 A).</td>
</tr>
<tr>
<td>Cables</td>
<td><strong>For Cisco Unified IP Phone 7975G, 7965G, and 7945G:</strong></td>
</tr>
<tr>
<td></td>
<td>• Category 3/5/5e/6 for 10-Mbps cables with 4 pairs</td>
</tr>
<tr>
<td></td>
<td>• Category 5/5e/6 for 100-Mbps cables with 4 pairs</td>
</tr>
<tr>
<td></td>
<td>• Category 5e/6 for 1000-Mbps cables with 4 pairs</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Cables have 4 pairs of wires for a total of 8 conductors.</td>
</tr>
<tr>
<td></td>
<td><strong>For Cisco Unified IP Phone 7971G-GE and 7970G:</strong></td>
</tr>
<tr>
<td></td>
<td>• Category 3/5/5e for 10-Mbps cables with 4 pairs</td>
</tr>
<tr>
<td></td>
<td>• Category 5/5e for 100-Mbps cables with 4 pairs</td>
</tr>
<tr>
<td></td>
<td>• Category 5e/6 for 1000-Mbps cables with 4 pairs</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Cables have 4 pairs of wires for a total of 8 conductors.</td>
</tr>
<tr>
<td>Distance requirements</td>
<td>As supported by the Ethernet specification, it is assumed that the maximum cable length between each Cisco Unified IP Phone and the switch is 100 meters (330 feet).</td>
</tr>
</tbody>
</table>
Cable Specifications

- RJ-9 jack (4-conductor) for handset and headset connection.
- RJ-45 jack for the LAN 10/100/1000BaseT connection (labeled 10/100/1000 SW).
- RJ-45 jack for a second 10/100/1000BaseT compliant connection (labeled 10/100/1000 PC).
- 3.5 mm jack for microphone and speaker connection (for Cisco Unified IP Phone 7971G-GE and 7970G only).
- 48-volt power connector.

Network and Access Port Pinouts

Although both the network and access ports are used for network connectivity, they serve different purposes and have different port pinouts. The access port is also known as the computer port.

Network Port Connector

The following table describes the network port connector pinouts.

<table>
<thead>
<tr>
<th>Pin number</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>BI_DA+</td>
</tr>
<tr>
<td>2</td>
<td>BI_DA-</td>
</tr>
<tr>
<td>3</td>
<td>BI_DB+</td>
</tr>
<tr>
<td>4</td>
<td>BI_DC+</td>
</tr>
<tr>
<td>5</td>
<td>BI_DC-</td>
</tr>
<tr>
<td>6</td>
<td>BI_DB-</td>
</tr>
<tr>
<td>7</td>
<td>BI_DD+</td>
</tr>
<tr>
<td>8</td>
<td>BI_DD-</td>
</tr>
</tbody>
</table>

*Note*  
BI stands for bidirectional, while DA, DB, DC and DD stand for Data A, Data B, Data C and Data D respectively.
Computer Port Connector

The following table describes the computer port connector pinouts.

**Table 61: Computer (Access) Port Connector Pinouts**

<table>
<thead>
<tr>
<th>Pin number</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>BI_DB+</td>
</tr>
<tr>
<td>2</td>
<td>BI_DB-</td>
</tr>
<tr>
<td>3</td>
<td>BI_DA+</td>
</tr>
<tr>
<td>4</td>
<td>BI_DD+</td>
</tr>
<tr>
<td>5</td>
<td>BI_DD-</td>
</tr>
<tr>
<td>6</td>
<td>BI_DA-</td>
</tr>
<tr>
<td>7</td>
<td>BI_DC+</td>
</tr>
<tr>
<td>8</td>
<td>BI_DC-</td>
</tr>
</tbody>
</table>

**Note** BI stands for bidirectional, while DA, DB, DC and DD stand for Data A, Data B, Data C and Data D respectively.

Phone Behavior During Times of Network Congestion

Anything that degrades network performance can affect phone voice and video 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
Basic Phone Administration Steps

- Phone Administration Overview, page 265
- Example User Information, page 265
- Cisco Unified Communications Manager User Addition, page 266
- Phone Setup, page 267
- Perform Final End User Setup, page 270

Phone Administration Overview

This appendix provides minimum, basic configuration steps for you to perform the following actions:

- Add a new user to Cisco Unified Communications Manager Administration
- Configure a new phone for that user
- Associate that user to that phone
- Complete other basic end-user configuration tasks

The procedures provide one method for performing these tasks and are not the only way to perform these tasks. They are a streamlined approach to get a new user and corresponding phone running on the system.

These procedures are designed to be used on a mature Cisco Unified Communications Manager system where calling search spaces, partitions, and other complicated configuration have already been done and are in place for existing users.

Example User Information

In the procedures that follow, examples are given when possible to illustrate some of the steps. Example user and phone information used throughout these procedures includes:

- User’s Name: John Doe
- User ID: johndoe
- MAC address listed on phone: 00127F576611
Cisco Unified Communications Manager User Addition

This section describes steps for adding a user to Cisco Unified Communications Manager. Follow one of the procedures in this section, depending on your operating system and the manner in which you are adding the user:

Add User from External LDAP Directory


If you added a user to an LDAP Directory (a non-Cisco Unified Communications Server directory), you can immediately synchronize that directory to the Cisco Unified Communications Manager on which you are adding this same user and the user phone by following these steps:

**Procedure**

1. Log onto Cisco Unified Communications Manager Administration.
3. Use the Find button to locate your LDAP directory.
4. Click on the LDAP directory name.
5. Click Perform Full Sync Now.
   
   **Note** If you do not need to immediately synchronize the LDAP Directory to Cisco Unified Communications Manager, the LDAP Directory Synchronization Schedule on the LDAP Directory window determines when the next autosynchronization occurs. However, the synchronization must occur before you can associate a new user to a device.

6. Proceed to Phone Setup, on page 267.

Add User Directly to Cisco Unified Communications Manager

If you are not using an LDAP directory, you can add a user directly to Cisco Unified Communications Manager Administration by following these steps:

**Procedure**

1. Choose User Management > End User, then click Add New. The End User Configuration window appears.
2. In the User Information pane of this window, enter the following:
• User ID: Enter the user identification name. Cisco Unified Communications Manager does not permit modifying the user ID after it is created. You may use the following special characters: =, +, <, >, #, ;, \, ”, ”, and blank spaces.

Example: johndoe

• Password and Confirm Password: Enter five or more alphanumeric or special characters for the end user password. You may use the following special characters: =, +, <, >, #, ;, \, ”, ”, and blank spaces.

• Last Name: Enter the user last name. You may use the following special characters: =, +, <, >, #, ;, \, ”, ”, and blank spaces.

Example: doe

• Telephone Number: Enter the primary directory number for the user. End users can have multiple lines on their phones.

Example: 26640 (John Doe’s internal company telephone number)

Step 3 Click Save.
Step 4 Proceed to the section Phone Setup, on page 267.

Phone Setup

To configure the phone, you must first identify the phone and then configure using the following procedures.

Identify Phone

To identify the user phone model and protocol, follow these steps:

Procedure

Step 1 From Cisco Unified Communications Manager administration, choose Device > Phone.
Step 2 Click Add New.
Step 3 Select the user phone model from the Phone Type drop-down list, then click Next.
Step 4 Select the device protocol (SCCP or SIP) from the drop-down list, then click Next. The Phone Configuration window appears.

Set Up Phone Fields

On the Phone Configuration window, you can use the default values for most of the fields.

To configure the required fields and some key additional fields, follow these steps:
Procedure

Step 1 For the required fields, possible values, some of which are based on the example of user johndoe, can be configured as follows:

a) In the Device Information pane of this window:

- MAC Address: Enter the MAC address of the phone, which is listed on a sticker on the phone. The MAC address is 12 hexadecimal characters long.

  Example: 00127F576611 (MAC address on John Doe’s phone)

- Description: This is an optional field in which you can enter a useful description, such as John Doe’s phone. This will help you if you need to search on information about this user.

- Device Pool: Choose the device pool to which you want this phone assigned. The device pool defines sets of common characteristics for devices, such as region, date/time group, softkey template, and MLPP information.

Note Device Pools are defined on the Device Pool Configuration window of Cisco Unified Communications Server Administration (System > Device Pool).

- Phone Button Template: Choose the appropriate phone button template from the drop-down list. The phone button template determines the configuration of buttons on a phone and identifies which feature is used for each button.

Note Phone button templates are defined on the Phone Button Template Configuration window of Cisco Unified Communications Manager Administration (Device > Device Settings > Phone Button Template). You can use the search fields in conjunction with the Find button to find all configured phone button templates and their current settings.

- Softkey Template: Choose the appropriate softkey template. The softkey template determines the configuration of the softkeys on Cisco Unified IP Phones. Leave this field blank if the common device configuration contains the assigned softkey template.

Note Softkey templates are defined on the Softkey Template Configuration window of Cisco Unified Communications Manager Administration (Device > Device Settings > Softkey Template). You can use the search fields in conjunction with the Find button to find all configured softkey templates and their current settings.

- Common Phone Profile: From the drop-down list box, choose a common phone profile from the list of available common phone profiles.

Note Common Phone Profiles are defined on the Common Phone Profile Configuration window of Cisco Unified Communications Manager Administration (Device > Device Settings > Common Phone Profile). You can use the search field in conjunction with the Find button to find all configured common phone profiles and their current settings.

- Calling Search Space: From the drop-down list box, choose the appropriate calling search space (CSS). A calling search space comprises a collection of partitions (analogous to a collection of available phone books) that are searched to determine how a dialed number should be routed. The calling search space for the device and the calling search space for the directory number get used together. The directory number CSS takes precedence over the device CSS.
**Calling Search Spaces** are defined on the Calling Search Space Configuration window of Cisco Unified Communications Manager Administration (**Calling routing** > **Class of Control** > **Calling Search Space**). You can use the search fields in conjunction with the **Find** button to find all configured Calling Search Spaces and their current settings.

- **Location:** Choose the appropriate location for this Cisco Unified IP Phone.
- **Owner User ID:** From the drop-down menu, choose the user ID of the assigned phone user.

b) In the Protocol Specific Information pane of this window, choose a Device Security Profile from the drop-down list. To enable security features for a phone, you must configure a new security profile for the device type and protocol and apply it to the phone. If the phone does not support security, choose a nonsecure profile. To identify the settings that are contained in the profile, choose **System > Security Profile > Phone Security Profile.**

**Note** The security profile chosen should be based on the overall security strategy of the company.

c) Also in the Protocol Specific Information pane of this window, choose the applicable SIP Profile from the drop-down list for SIP phones.

d) In the Extension Information pane of this window, check the Enable Extension Mobility box if this phone supports Cisco Extension Mobility.

e) In the Product Specific Configuration Layout pane of this window, enable the Video Capabilities field if this field appears on your window.

f) Click **Save.**

### Step 2

Configure line settings:

a) On the Phone Configuration window, click Line 1 on the left pane of the window. The Directory Number Configuration window appears.

b) In the Directory Number field, enter a valid number that can be dialed.

**Note** This field should contain the same number that appears in the Telephone Number field on the User Configuration window.

**Example:** 26640 is the directory number of user John Doe in the example above.

c) From the Route Partition drop-down list, choose the partition to which the directory number belongs. If you do not want to restrict access to the directory number, choose <None> for the partition.

d) From the Calling Search Space drop-down list (Directory Number Settings pane of the Directory Number Configuration window), choose the appropriate calling search space. A calling search space comprises a collection of partitions that are searched for numbers that are called from this directory number. The value that you choose applies to all devices that are using this directory number.

e) In the Call Pickup and Call Forward Settings pane of the Directory Number Configuration window, choose the items (for example, Forward All, Forward Busy Internal) and corresponding destinations to which calls should be sent.

**Example:** If you want incoming internal and external calls that receive a busy signal to be forwarded to the voice mail for this line, check the Voice Mail box next to the “Forward Busy Internal” and “Forward Busy External” items in the left column of the Call Pickup and Call Forward Settings pane.

f) In the “Line 1 on Device...” pane of the Directory Number Configuration window, configure the following fields:

- **Display (Internal Caller ID field):** You can enter the first name and last name of the user of this device so that this name is displayed for all internal calls. You can also leave this field blank to have the system display the phone extension.
• External Phone Number Mask: Indicate phone number (or mask) that is used to send Caller ID information when a call is placed from this line.

You can enter a maximum of 24 number and "X" characters. The Xs represent the directory number and must appear at the end of the pattern.

Example: Using the john doe extension in the example above, if you specify a mask of 408902XXXX, an external call from extension 6640 displays a caller ID number of 4089026640.

Note This setting applies only to the current device unless you check Update Shared Device Settings and click Propagate Selected. The check box at right displays only if other devices share this directory number.

g) Click Save.
h) Click Associate End Users at the bottom of the window to associate a user to the line being configured. Use the Find button in conjunction with the Search fields to locate the user, then check the box next to the name, and then click Add Selected. The name and user ID should now appear in the "Users Associated With Line" pane of the Directory Number Configuration window.
i) Click Save. The user is now associated with Line 1 on the phone.
j) If the phone has a second line, configure Line 2.
k) Associate the user with the device:

• Choose User Management > End User.

• Use the search boxes and the Find button to locate the user you have added (for example, Doe for the last name).

• Click on the user ID (for example, johndoe). The End User Configuration window appears.

• Click Device Associations.

• Use the Search fields and the Find button to locate the device with which you want to associate to the user.

• Select the device, then click Save Selected/Changes. The user is now associated with the device.

• Click Go next to the Back to User link in the upper-right corner of the screen.

Step 3 Proceed to Perform Final End User Setup, on page 270.

Perform Final End User Setup

If you are not already on the End User Configuration page, choose User Management > End User to perform some final configuration tasks. Use the Search fields and the Find button to locate the user (for example, John Doe), then click on the user ID to get to the End User Configuration window for the user.

In the End User configuration window, do the following:
Procedure

Step 1  In the Directory Number Associations pane of the screen, set the primary extension from the drop-down list.
Step 2  In the Mobility Information pane, check **Enable Mobility**.
Step 3  In the Permissions Information pane, use the User Group buttons to add this user to any user groups. For example, you may want to add the user to a group that has been defined as a “Standard CCM End User Group.” To view all configured user groups, choose **User Management > User Group**.
Step 4  Click **Save**.
Perform Final End User Setup
INDEX

.cnf.xml configuration file 34
"more" Softkey Timer 93

10/100 PC port 45
   See also access port
10/100 SW port 45
   See also network port
10/100/1000 PC port 45
   See also access port
10/100/1000 SW port 45
   See also network port
802.1X 6, 21, 22
   authentication 22
   authentication server 22
   authenticator 22
   description 6
   network components 22
   supplicant 22
802.1X Authentication 109
802.1X authentication and status 116
802.1X Authentication menu 116
   options 116
   Device Authentication 116
   EAP-MD5 116
802.1X Authentication Status menu 109, 116
   about 109
   states 116

A

abbreviated dialing 124, 249
AC adapter 48
   connecting 48
access 59, 62
   to phone settings 59, 62
access port 45, 48, 66, 100, 101
   10/100 PC 45
   10/100/1000 PC 45
   configuring 66

access port (continued)
   connecting 48
   disabled 101
   forwarding packets to 100
access to phone settings 61
Access web page 200, 208
adding 38, 39, 40, 156
   Cisco Unified IP Phones manually 39
   Cisco Unified IP Phones using auto-registration 38
   Cisco Unified IP Phones using BAT 40
   users to Cisco Unified Communications Manager 156
Address Book Synchronization Tool (TABSync) 246, 247
   configuring 247
   installing 247
   obtaining 246
Admin. VLAN ID 66
Advance Adhoc Conference service parameter 124
agent greeting 124, 249
Alternate TFTP 66
anonymous call block 124, 249
answer release 249
any call pickup 124
Any Call Pickup 124
assisted directed call park 124, 249
Audible message waiting indicator 124, 249
authenticated call 18
authentication 13, 58
authentication server 22
   in 802.1X 22
Authentication URL 90
authenticator 22
   in 802.1X 22
auto answer 124, 249
Auto Call Select 93
auto dial 124, 249
Auto Line Select 93
auto-pickup 124, 249
auto-registration 38
   using 38
automatic port synchronization 124, 249
auxiliary VLAN 30
B
background image 170, 171
  configuring 171
  creating 170
  custom 170
  List.xml file 170
  PNG file 170, 171
barge 23, 124, 249
BAT (Bulk Administration Tool) 40
block external to external transfer 124, 249
BootP 6
BOOTP Server 66
Bootstrap Protocol (BootP) 6
Busy Lamp Field (BLF) 93, 124, 249
call lists 93
call pickup 124, 249
callforward 124, 249
  all breakout 249
  all calls 124, 249
  all loop prevention 249
  busy 249
  configurable display 249
  destination override 124
  display, configuring 124
  loop breakout 124
  loop prevention 124
  no answer 249
  call forward display 124
    configuring 124
  call park 124, 249
  call pickup 124, 249
  Call Preferences menu 89
call recording 124
  Call Statistics screen 177, 193
call waiting 124, 249
caller ID 124, 249
caller ID blocking 249
calling party normalization 124
  CAPF (Certificate Authority Proxy Function) 15, 59
  CDP 21
  Certificate Trust List 13
  Cisco Catalyst Switch 22
  Cisco Discovery Protocol, See CDP
  Cisco Extension Mobility Change PIN 124
  Cisco Extension Mobility Cross Cluster (EMCC) 124
  Cisco Extension Mobility Cross Cluster Service 249
  Cisco Peer to Peer Distribution Protocol (CPPDP) 6
  Cisco Secure Access Control Server (ACS) 22
  Cisco Unified Communications Manager 30, 37, 44, 220
    adding phone to database of 37
    interactions with 30
    required for Cisco Unified IP Phones 44
    verifying settings 220
  Cisco Unified Communications Manager Administration 124, 174
    adding telephony features using 124
    configuring LCD display using 174
  Cisco Unified Communications Manager Assistant 124, 249
  Cisco Unified IP Phone 2, 6, 23, 24, 26, 31, 37, 38, 39, 40, 48, 55, 151,
    152, 155, 199, 217, 236, 241, 261
    adding manually to Cisco Unified Communications Manager 39
    adding to Cisco Unified Communications Manager 37
    cleaning 241
    configuration checklist 24
    configuration requirements 23
    configuring user services 155
    features 2
    figure 2
    installation checklist 26
    installation overview 23
    installation procedure 48
    installation requirements 23
    modifying phone button templates 152
    mounting to wall 55
    power sources 31
    registering 37
    registering with Cisco Unified Communications Manager 38, 40
    resetting 236
    supported networking protocols 6
    technical specifications 261
    troubleshooting 217
    using LDAP directories 151
    web page 199
  Cisco Unified IP Phone Expansion Module 50, 179, 192, 236
    statistics 179, 192
    troubleshooting 236
  cleaning the Cisco Unified IP Phone 241
  Clear softkey 179, 188
  client matter codes 124, 249
computer telephony integration (CTI) 124, 249
conference 18, 124
See also secure conference
secure 18
See also secure conference
conference joining 124
configurable call forward display 249
Configuration 159
Power Save 159
configuration file 15, 34, 220
.cnf.xml 34
creating 220
encrypted 15
overview 34
secure 34
XmlDefault.cnf.xml 34
Configuration Parameters 150
configuring 23, 58, 63, 151, 152, 155, 156, 159
from a Cisco Unified IP Phone 63
LDAP directories 151
overview 23
personal directories 151
phone button templates 152
Power Save 159
softkey templates 155
startup network settings 58
user features 156
connecting 48
handset 48
headset 48
to a computer 48
to AC adapter 48
to the network 48
Console Logs web page 200
Core Dumps web page 200
CTL 224
troubleshooting 224
CTL file 36, 237
deleting from phone 237
requesting 36
CTL File menu 111
CTL File screen 111
custom phone rings 168, 169, 171
about 168
creating 168, 169, 171
PCM file requirements 169

d

daisy chaining 233
data VLAN 30
Days Display Not Active 99, 174

E

EAP-MD5 116
  Device ID 116
  Realm 116
  Shared Secret 116
editing 63
  configuration values 63
encrypted call 18
encrypted configuration file 15
encryption 13, 15
  media 13, 15
  signaling 13, 15
EnergyWise 23, 159
  configuration 159
  description 23
Erase softkey 237
error messages 219
  used for troubleshooting 219
Ethernet Configuration menu 100
  about 100
  Span to PC Port option 100
Ethernet Information web page 200, 208
Expansion Module, See Cisco Unified IP Phone Expansion Module
Expansion Module(s) screen 179
Expansion Modules screen 192
extension mobility 249

features (continued)
support by protocol (continued)
  Busy Lamp Field (BLF) 249
call back 249
  Call Back 249
call display restrictions 249
call forward 249
call park 249
call pickup 249
call waiting 249
caller ID 249
caller ID blocking 249
Cisco Unified Communications Manager Assistant 249
client matter codes 249
computer telephony integration (CTI) Applications 249
configurable call forward display 249
direct transfer 249
directed call park 249
distinctive ring 249
DND 249
extension mobility 249
fast dial service 249
forced authorization codes 249
group call pickup 249
Help system 249
hold 249
hold reversion 249
immediate divert 249
Immediate divert enhanced 249
intercom 249
join 249
join across lines 249
log out of hunt groups 249
malicious caller identification (MCID) 249
meet-me conference 249
message waiting 249
mobile connect 249
mobile voice access 249
multilevel precedence and preemption (MLPP) 249
music-on-hold 249
mute 249
on-hook dialing 249
onhook call transfer 249
other group pickup 249
pickup 249
presence-enabled directories 249
privacy 249
Private Line Automated Ringdown (PLAR) 249
programmable line keys 249
protected calling 249
Quality Reporting Tool (QRT) 249
redial 249
ring setting 249
secure conference 249

features (continued)
support by protocol (continued)
   Services URL button 249
   shared line 249
   single button barge 249
   speed dialing 249
   Time-of-Day Routing 249
touchscreen illumination disabling 249
   transfer 249
   transfer-direct transfer 249
   URL dialing 249
   video mode 249
   video support 249
   voice mail 249
   web dialer 249
figure 2
Cisco Unified IP Phone features 2
file authentication 15
file format 168, 170
   List.xml 170
   RingList.xml 168
firmware 191
   verifying version 191
Firmware Versions screen 191
footstand 4
   button for 4
forced authorization codes 124, 249

G
G.711a 1
G.711mu 1
G.722 1
G.722 codec 96
G.729 1
G.729a 1
G.729ab 1
G.729b 1
GARP Enabled 101
group call pickup 124, 249

H
handset 4, 48
   connecting 48
   light strip 4
headset 46, 47, 48
   audio quality 46, 48
   connecting 47
   disabling 47
   quality 48
headset (continued)
   using 46
   wireless, enabling 47
Headset 4
   button 4
Headset Enabled 96
headset port 48
Help button 4
help system 124
Help system 249
hold 124, 249
hold reversion 124, 249
hold status 124
hookswitch clip 45
   removing 45
Host Name 66
HTTP 6, 202
   description 6
HTTP Configuration menu 90
   about 90
   Authentication URL 90
   Directories URL 90
   Idle URL 90
   Idle URL Time 90
   Information URL 90
   Messages URL 90
   Proxy Server URL 90
   Services URL 90
HTTPS 202
hunt group 124
   log out of hunt groups 124
   hunt group display 124, 249
Hypertext Transfer Protocol (HTTP) 6
   description 6

I
icon 18
   lock 18
   padlock 18
   shield 18
idle display 90, 173
   configuring 173
   timeout 90
   viewing settings 173
   XML service 90, 173
Idle URL 90
Idle URL Time 90
iLBC 1
iLBC codec 233
image authentication 15
immediate divert 124, 249
Immediate divert enhanced 124, 249
Information URL 90
installing 23, 37, 44, 48
Cisco Unified Communications Manager configuration 44
network requirements 44
preparing 37
procedure 48
requirements, overview 23
intercom 124, 249
interference 1
mobile phone 1
Internet Protocol (IP) 6
Intra-Cluster Trust 249
IP address 219
troubleshooting 219
IP Address 66
IPv4 Configuration 66
IPv6 Address 66
IPv6 Alternate TFTP 66
IPv6 Configuration 66
IPv6 Default Router 1-2 66
IPv6 DNS Server 1-2 66
IPv6 Load server 103
IPv6 Log server 103
IPv6 on the Cisco Unified IP Phone 11
IPv6 Prefix Length 66
IPv6 TFTP Server 1 66
IPv6 TFTP Server 2 66

J
join 124, 249
join across lines 124, 249

K
keypad 4

L
language overlays 259
LCD screen 174
turning on and off automatically 174
LDAP directories 151
using with Cisco Unified IP Phone 151
line buttons 4
Line Select 124
Line select for voice messages 124
Line Settings menu 88
lines 4
buttons 4
Link Layer Discovery Protocol (LLDP) 203
network configuration 203
Link Layer Discovery Protocol-Media Endpoint Devices (LLDP-MED) 203
network configuration 203
List.xml file 170
Locale Configuration menu 92, 93
about 92, 93
Network Locale 92
Network Locale Version 92
User Locale 92
User Locale Char Set 92
User Locale Version 92
localization 259
phone button overlays for 259
lock icon 18
log out of hunt groups 249
Log server 103
IPv6 Log server 103
Logging Display 101

M
MAC address 66
malicious caller identification (MCID) 124, 249
manufacturing installed certificate (MIC) 15
Media Configuration menu 96
about 96
options 96
Headset Enabled 96
Recording Tone 96
Recording Tone Duration 96
Recording Tone Local Volume 96
Recording Tone Remote Volume 96
Speaker Enabled 96
Video Capability Enabled 96
media encryption 15
Meet Me conference 124
meet-me conference 249
message waiting 124, 249
Messages button 4
Messages URL 90
metrics 211
voice quality 211
MIC 15
missed call logging 124
mobile connect 124, 249
mobile phone interference 1
mobile voice access 124, 249
Model Information screen 177
multilevel precedence and preemption (MLPP) 124, 249
multiple calls per line appearance 124
music-on-hold 124, 249
mute 124, 249
    feature 124, 249
Mute button 4

N

native VLAN 30
Navigation button 4
Network Configuration Area items 203
    LLDP on PC port 203
    LLDP-MED on SW port 203
Network Configuration menu 61, 62, 63, 66, 103, 196
    about 66
    displaying 62
    editing values 63, 196
IPv4 66
    Alternate TFTP 66
    BootP Server 66
    Default Router 1-5 66
    DHCP 66
    DHCP Address Released 66
    DHCP Server 66
    DNS Server 1-5 66
    IP Address 66
    Subnet Mask 66
    TFTP Server 1 66
    TFTP Server 2 66
IPv6 66
    DHCPv6 66
    DHCPv6 Address Released 66
    IPv6 Address 66
    IPv6 Alternate TFTP 66
    IPv6 Default Router 1-6 66
    IPv6 DNS Server 1-2 66
    IPv6 Prefix Length 66
    IPv6 TFTP Server 1 66
    IPv6 TFTP Server 2 66
locking options 63
options 66, 103
    Admin. VLAN ID 66
    CDP on PC port 103
    CDP on switch port 103
    Domain Name 66
    Host Name 66
    MAC Address 66
    Operational VLAN ID 66
    PC Port Configuration 66
    PC VLAN 66
    SW Port Configuration 66

Network Configuration menu (continued)
    overview 61
    unlocking options 63
Network Configuration web page 200, 203
    network connectivity 219
    verifying 219
Network Locale 92
Network Locale Version 92
network outages 222
    identifying 222
    network requirements 44
        for installing 44
    network settings 58
        startup configuration 58
    network statistics 188, 208
Network Statistics screen 188
Network web page 200, 208
networking protocol 6
    802.1X 6
    BootP 6
    CDP 6
    CPPDP 6
    DHCP 6
    HTTP 6
    IP 6
    RTCP 6
    RTP 6
    SCCP 6
    SIP 6
    TCP 6
    TFTP 6
    TLS 6
    UDP 6
networking protocols 6
    supported 6

O

on-hook dialing 249
onhook call transfer 124, 249
onhook predialing 124
Operational VLAN ID 66
other group pickup 124, 249
padlock icon 18, 63, 196
PC 45
  connecting to the phone 45
PC Port Configuration 66
PC Port Disabled 101
PC VLAN 66
PCM file requirements 169
  for custom ring types 169
Peer firmware sharing 103
personal directories 151
phone button templates 152
phone screen 4, 32
phone screen illumination disabling 124
phone secure web access 124
phone settings access 61
physical connection 222
  verifying 222
plugging in Cisco Unified IP Phone 48
  plus dialing 124, 249, 260
PNG file 170, 171
power 23, 31, 32, 34, 159
  EnergyWise 23
  EnergyWise configuration 159
  EnergyWise description 23
  maximum required from a switch 32
  outage 34
  providing to the Cisco Unified IP Phone 31
  power consumption 32
Power over Ethernet (PoE) 31
Power Save Configuration menu 99
  about 99
  options 99
    Days Display Not Active 99
    Display Idle Timeout 99
    Display On Duration 99
    Display On Time 99
    Display On When Incoming call 99
power source 31, 32, 224
  causing phone to reset 224
  description 31
  effect on phone screen brightness 32
  external power 31
  PoE 31
  power consumption 32
  power injector 31
presence-enabled directories 124, 249
privacy 124, 249
Private Line Automated Ringdown (PLAR) 124, 249
programmable buttons 4
  description 4
programmable line keys 124, 249
protected call 18, 19
  description 19
protected calling 124, 249
  all calls 249
  description 124
Protected Calls 19
Proxy Server URL 90
QoS Configuration menu 102
  about 102
  options 102
    DSCP For Call Control 102
    DSCP For Configuration 102
    DSCP For Services 102
QRT softkey 124, 239
Quality Reporting Tool (QRT) 124, 239, 249
Real-Time Control Protocol, See RTCP
Real-Time Transport Protocol, See RTP
Recording Tone 96
Recording Tone Duration 96
Recording Tone Local Volume 96
Recording Tone Remote Volume 96
redial 124, 249
reset 237
  basic 237
  factory 237
resetting 222, 223, 236, 237
  basic 237
  Cisco Unified IP phone 236
  continuously 222
  intentionally 223
  methods 237
ring activity 124
ring setting 249
ringer 4
  indicator 4
  ringer volume control 124, 249
RingList.xml file format 168
SCCP 6
  description 6
  screen, See LCD screen
secure and nonsecure indication tone 124, 249
secure conference 18, 19, 124, 249
description 18, 124
establishing 18
identifying 18
restrictions 19
secure SRST reference 15
securing the phone with a cable lock 53
security 15, 17, 34, 58, 59
CAPF (Certificate Authority Proxy Function) 15, 59
configuring on phone 58
device authentication 15
encrypted configuration file 15
file authentication 15
image authentication 15
Locally Significant Certificate (LSC) 58
manufacturing installed certificate (MIC) 15
media encryption 15
secure configuration file 34
secure SRST reference 15
security profiles 15, 17
signaling authentication 15
signaling encryption 15
Security Configuration menu 119
options 119
VPN Client 119
Security Configuration menu (on Device Configuration menu) 101
about 101
options 101
GARP Enabled 101
Logging Display 101
PC Port Disabled 101
Security Mode 101
Voice VLAN Enabled 101
Web Access Enabled 101
Security Configuration menu (on Settings menu) 109
about 109
options 109
802.1X Authentication 109
802.1X Authentication Status 109
LSC 109
MIC 109
Security Mode 109
Trust List 109
Web Access Enabled 109
Security Mode 101
security profiles 15, 17
Select button 4
services 124, 155, 249
configuring for users 155
description 124
protocol support 249
subscribing to 155
Services button 4
Services URL 90
Services URL button 124, 249
session handoff 124
Session Handoff 249
Settings button 4
Settings menu access 59, 62
shared line 124, 249
shield icon 18
sidetone level 249
signaling authentication 15
signaling encryption 15
silent monitoring 124, 249
single button barge 124, 249
SIP 6
description 6
SIP Configuration menu 87
SIP General Configuration menu 87
softkey buttons 4
description 4
softkey templates 155
configuring 155
Span to PC Port 100
Speaker 4
button 4
Speaker button 45
disable 45
Speaker Enabled 96
speed dial 152
template for 152
Speed Dial 4
buttons 4
speed dialing 124, 249
SRST 15, 85, 203
secure reference 15
standard (ad hoc) conference 124
startup problems 217
startup process 36, 57
accessing TFTP server 36
configuring VLAN 36
contacting Cisco Unified Communications Manager 36
loading stored phone image 36
obtaining IP address 36
obtaining power 36
requesting configuration file 36
requesting CTL file 36
understanding 36
verifying 57
statistics 188, 193, 208, 211
call 193
network 188, 208
streaming 211
Status menu 177, 179
description 177
Status menu (continued)
  submenus on 179
status messages 179
Status Messages screen 179
Status Messages web page 200, 211
Stream 0 web page 211
Stream 1 web page 200, 211
Stream 2 web page 200, 211
Stream 3 web page 200, 211
streaming statistics 211
Subnet Mask 66
supplicant 22
  in 802.1X 22
Survivable Remote Site Telephony, See SRST
SW Port Configuration 66
troubleshooting (continued)
  Cisco Unified IP Phone Expansion Module 236
  DHCP 222
  DNS 224
  DNS settings 219
  IP addressing and routing 219
  network connectivity 219
  network outages 222
  phones resetting 223
  physical connection 222
  services on Cisco Unified Communications Manager 220
  TFTP settings 219
  VLAN configuration 223
Trust List menu 115

T

TABSynch 246, 247
  configuring 247
  installing 247
  obtaining 246
TCP 6
  technical specifications 261
  for Cisco Unified IP Phone 261
telephony features 23, 103, 249
  barge 23
  IPv6 Log server 103
  Log server 103
  Peer firmware sharing 103
  VPN client 249
TFTP 6, 219
  description 6
  troubleshooting 219
TFTP Server 1 66
TFTP Server 2 66
TFTP settings 13
time 44
  displayed on phone 44
time zone update 124, 249
Time-of-Day Routing 124, 249
TLS 34
touchscreen, See LCD screen
touchscreen illumination disabling 124, 249
transfer 249
transfer-direct transfer 249
Transmission Control Protocol, See TCP
Transport Layer Security, See TLS
Trivial File Transfer Protocol, See TFTP
troubleshooting 217, 219, 220, 222, 223, 224, 236
  Cisco Unified Communications Manager settings 220
  Cisco Unified IP Phone 217

UCR 2008 124, 162, 221
  description 124
  POST update error 221
  Security Error 221
  Setting up 162
UI Configuration menu 93
  options 93
    Auto Call Select 93
    Auto Line Select 93
    BLF for call lists 93
uncompressed wideband 1
Understanding DHCPv6 and Autoconfiguration 84
Unified CM 1-5 85
Unified CM Configuration menu 85
URL dialing 249
User Datagram Protocol, See UDP
User Locale 92
User Locale Char Set 92
User Locale Version 92
User Options web page 157, 158, 244
  description 157
  giving users access to 157, 244
  specifying options that appear 158
users 156, 243, 244, 245, 246
  accessing voice messaging system 246
  adding to Cisco Unified Communications Manager 156
  configuring personal directories 246
  documentation for 244
  providing support to 243
  required information 243
  subscribing to services 245
using phone templates to add phones 40
V

verifying 57
  startup process 57
Video Capability Enabled 96
video mode 124, 249
video support 124, 249
VLAN 30, 66, 223
  auxiliary, for voice traffic 30
  configuring 66
  configuring for voice networks 30
  native, for data traffic 30
  verifying 223
voice mail 249
voice messaging system 124, 246
  accessing 246
voice quality metrics 211
voice VLAN 30
Voice VLAN Enabled 101
Volume button 4
VPN client 124, 249
VPN Client 119
VPN configuration 119
VPN support in phones 249

W

wall mounting 55
  Cisco Unified IP Phone 55
Web Access Enabled 101
web dialer 249

X

XmlDefault.cnf.xml 34