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

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

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

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

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

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

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

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

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOSS 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
- Overview xiii
- Audience xiii
- Organization xiv
- Related Documentation xv
  - Cisco Unified IP Phone 7900 Series Documentation xv
  - Cisco Unified Communications Manager Documentation xv
  - Cisco Business Edition 5000 Documentation xv
- Documentation, Support, and Security Guidelines xv
- Cisco Product Security Overview xv
- Guide Conventions xvi

## CHAPTER 1
- Cisco Unified IP Phones 1
  - Phone Overview 1
  - Cisco Unified IP Phone 7906G and 7911G 2
    - Buttons and Hardware 2
  - Network Protocols 3
    - IPv6 Support on Cisco Unified IP Phones 8
  - Cisco Unified IP Phone 7906 and 7911 Supported Features 8
    - Feature Overview 8
    - Telephony Feature Administration 9
    - Cisco Unified IP Phone Network Parameters 9
    - Information for End Users 9
  - Cisco Unified IP Phone Security Features 10
    - Supported Security Features 12
    - Security Profiles 14
    - Authenticated, Encrypted, and Protected Phone Calls 14
Secure Conference Call Identification 15
Protected Call Identification 16
Call Security Interactions and Restrictions 16
802.1X Authentication 18
   Overview 18
   Required Network Components 18
   Best Practices, Requirements, and Recommendations 19
UCR 2008 20
Security Restrictions 20
Phone Power Consumption 21
Cisco Unified IP Phone Deployment 21
   Cisco Unified IP Phone Setup in Cisco Unified Communications Manager 21
   Set Up Cisco Unified IP Phones 7906G and 7911G in Cisco Unified Communications
   Manager 22
   Cisco Unified IP Phone Installation 24
   Install Cisco Unified IP Phones 7906G and 7911G 25

CHAPTER 2
Cisco Unified IP Phones and Telephony Networks 27
   Phone and Telephony Network Overview 27
   Cisco Unified Communications Product Interactions 27
      Cisco Unified IP Phone and Cisco Unified Communications Manager Interaction 28
      Cisco Unified IP Phones and VLAN Interaction 28
   Cisco Unified IP Phone Power 29
      Power Guidelines 29
      Power Outage 30
      Additional Information About Power 30
   Phone Configuration Files 31
      SIP Dial Rules 31
   Phone Startup Process 32
   Cisco Unified Communications Manager Phone Addition Methods 33
      Autoregistration Phone Addition 33
      Autoregistration and TAPS Phone Addition 34
      Cisco Unified Communications Manager Administration Phone Addition 35
      Add Phones with BAT 35
   Cisco Unified IP Phones and Different Protocols 36
Contents

CHAPTER 3
Cisco Unified IP Phone Installation
  Phone Installation Overview
  Before You Begin
    Network Requirements
    Cisco Unified Communications Manager Setup
  Cisco Unified IP Phones 7906G and 7911G Components
    Network and Access Ports
    Handset
    Speaker
      Disable Speakerphone
      Monitor Mode
      Group Listen Mode
        Set Up Group Listen Mode on Cisco Unified Communications Manager
        Group Listen Activation on Phone
    Headset
      Audio Quality
      Headset Connection
      External Device Use
  Install Cisco Unified IP Phones
    Footstand Installation
  Cisco Unified IP Phone 7906G Installation
  Cisco Unified IP Phone 7911G Installation
  Mount Phone on Wall
  Phone Startup Verification
  Network Settings
  Cisco Unified IP Phone Security
    Install Locally Significant Certificate

CHAPTER 4
Cisco Unified IP Phone Settings
  Phone Settings Overview
Cisco Unified IP Phones 7906G and 7911G Menus 53
   Display Settings Menu 54
   Unlock and Lock Options 55
   Value Input Guidelines 55
Phone Setup Options 56
Network Configuration Menu 57
   Set IPv4 Configuration Fields 63
   Set Domain Name Field 64
   Set Admin VLAN ID Field 64
   Set SW Port Configuration Field 65
   Set PC Port Configuration Field 65
   Set PC VLAN Field 66
   Set DHCP Field 66
   Set IP Address Field 66
   Set Subnet Mask Field 67
   Set Default Router Fields 67
   Set DNS Server Fields 67
   Set DHCP Address Released Field 68
   Set Alternate TFTP Field 68
   Set TFTP Server 1 Field 68
   Set TFTP Server 2 Field 69
Device Configuration Menu 69
   Unified CM Configuration Menu 69
   SIP Configuration Menu for SIP Phones 70
      SIP General Configuration Menu 70
      Line Settings Menu for SIP Phones 72
   Call Preferences Menu for SIP Phones 73
   HTTP Configuration Menu 74
   Locale Configuration Menu 75
   UI Configuration Menu 76
   Media Configuration Menu 78
   NTP Configuration Menu for SIP Phones 79
   Ethernet Configuration Menu 79
   Security Configuration Menu 80
   QoS Configuration Menu 82
CHAPTER 5

Features, Templates, Services, and Users 97

Features, Templates, Services, and Users Overview 97

Telephony Features Available for Cisco Unified IP Phone 98

Set Up Enbloc Dialing Feature 117

Set Up Secure and Nonsecure Indication Tone Feature 117

Set Up SSH Access Feature 118

Product-Specific Parameters 118

Corporate and Personal Directory Setup 119

Corporate Directory Setup 119

Personal Directory Setup 120

Phone Button Templates 120

Modify Phone Template 120

Phone Button Template for Personal Address Book or Fast Dials 121

Set Up PAB or Fast Dial in IP Phone Services 121

Change Phone Button Template for PAB or Fast Dial 122

Softkey Templates 123

Enable Device Invoked Recording 123

Services Setup 124

Cisco Unified Communications Manager User Addition 124

User Options Web Pages Management 125

User Access to User Options Web Pages 125

Add User to End User Group 125

Associate Phones with Users 126

Customize User Options Web Page Display 126

EnergyWise Setup on Cisco Unified IP Phone 127
CHAPTER 8
Remote Monitoring 163

Remote Monitoring Overview 163
Access Web Page for Phone 164
Phone Web Page Overview 164
Control Web Page Access 165
Cisco Unified IP Phone and HTTP or HTTPS Protocols 166
Device Information Area 166
Network Configuration Area 167
Network Statistics Area 171
Ethernet Information Area Fields 172
Access and Network Area Fields 172
Device Logs Area 174
Streaming Statistics 175

CHAPTER 9
Troubleshooting and Maintenance 179

Troubleshooting and Maintenance Overview 179
Troubleshooting 179
Startup Problems 179
Cisco Unified IP Phone Does Not Go Through Normal Startup Process 179
Cisco Unified IP Phone Does Not Register with Cisco Unified Communications Manager 180
Phone Displays Error Messages 180
Cisco Unified Communications Manager Phone Registration 181
Phone Cannot Connect to TFTP Server or to Cisco Unified Communications Manager 181
TFTP Server Settings 181
IP Address and Routing 182
DNS Settings 182
Cisco Unified Communications Manager Settings on Phone 182
Cisco CallManager and TFTP Services Are Not Running 182
Start Service 193
Create New Configuration File 194
Determine DNS or Connectivity Issues 195
General Troubleshooting Information 195
Cisco Unified IP Phone Reset or Restore 197
Basic Reset 197
Perform Factory Reset 198
Additional Troubleshooting Information 199
Maintenance 199
Quality Report Tool 199
Voice Quality Monitoring 199
Voice Quality Metric Interpretation 200
Voice Quality Troubleshooting Tips 201
Cisco Unified IP Phone Cleaning 201

APPENDIX A

Internal Support Web Site 203
Internal Support Web Site Overview 203
Cisco Unified IP Phone User Support 203
User Options Web Pages Access 204
Cisco Unified IP Phone Manuals 204
Cisco Unified IP Phone 7900 Series eLearning Tutorials for SCCP Phones 204
Phone Features User Subscription and Setup 205
User Voice Messaging System Access 205
User Personal Directory Entries Setup 206
Obtain Cisco Unified IP Phone Address Book Synchronizer 206
Cisco Unified IP Phone Address Book Synchronizer Deployment 206
Install Synchronizer 207
Set Up Synchronizer 207

APPENDIX B

Feature Support by Protocol for Cisco Unified IP Phone 209

APPENDIX C

International User Support 217
International User Support Overview 217
Unified Communications Manager Endpoints Locale Installer 217
Language Limitation 218
International Call Logging Support 218

---

**APPENDIX D**

**Technical Specifications** 219
- Physical and Operating Environment Specifications 219
- Cable Specifications 220
- Network and Access Port Pinouts 220
  - Network Port Connector 220
  - Computer Port Connector 221
- Phone Behavior During Times of Network Congestion 222

---

**APPENDIX E**

**Basic Phone Administration Steps** 223
- Phone Administration Overview 223
- Example User Information 223
- Cisco Unified Communications Manager User Addition 224
  - Add User from External LDAP Directory 224
  - Add User Directly to Cisco Unified Communications Manager 224
- Phone Setup 225
  - Identify Phone 225
  - Set Up Phone Fields 225
- Perform Final End User Setup 228
Preface

- Overview, page xiii
- Audience, page xiii
- Organization, page xiv
- Related Documentation, page xv
- Documentation, Support, and Security Guidelines, page xv
- Cisco Product Security Overview, page xv
- Guide Conventions, page xvi

Overview

Cisco Unified IP Phone 7906G and 7911G Administration Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP) provides the information you need to understand, install, configure, manage, and troubleshoot the Cisco Unified IP Phones 7906G and 7911G in a Voice over IP (VoIP) network.

This guide does not provide complete configuration information or procedures for Cisco Unified Communications Manager or other associated network infrastructure.

Related Topics

- Related Documentation, on page xv

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.
## Organization

This manual is organized as follows:

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified IP Phones, on page 1</td>
<td>Provides a conceptual overview and description of the Cisco Unified IP Phones.</td>
</tr>
<tr>
<td>Cisco Unified IP Phones and Telephony Networks, on page 27</td>
<td>Describes how the Cisco Unified IP Phones interacts with other key Unified Communications components, and provides an overview of the tasks required prior to installation.</td>
</tr>
<tr>
<td>Cisco Unified IP Phone Installation, on page 39</td>
<td>Describes how to properly and safely install and configure the Cisco Unified IP Phones on your network.</td>
</tr>
<tr>
<td>Cisco Unified IP Phone Settings, on page 53</td>
<td>Describes how to configure network settings, verify status, and make global changes to the Cisco Unified IP Phones.</td>
</tr>
<tr>
<td>Features, Templates, Services, and Users, on page 97</td>
<td>Provides an overview of procedures for configuring telephony features, configuring directories, configuring phone button and softkey templates, setting up services, and adding users to Cisco Unified Communications Manager.</td>
</tr>
<tr>
<td>Cisco Unified IP Phone Customization, on page 135</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 143</td>
<td>Explains how to view model information, status messages, network statistics, and firmware information from the Cisco Unified IP Phones.</td>
</tr>
<tr>
<td>Remote Monitoring, on page 163</td>
<td>Explains how to obtain status information about the phone using the phone’s web page.</td>
</tr>
<tr>
<td>Troubleshooting and Maintenance, on page 179</td>
<td>Provides tips for troubleshooting the Cisco Unified IP Phones.</td>
</tr>
<tr>
<td>Internal Support Web Site, on page 203</td>
<td>Provides suggestions for setting up a website for providing users with important information about their Cisco Unified IP Phones.</td>
</tr>
<tr>
<td>Feature Support by Protocol for Cisco Unified IP Phone, on page 209</td>
<td>Provides information about feature support for the Cisco Unified IP Phones using the SCCP or SIP protocol.</td>
</tr>
<tr>
<td>International User Support, on page 217</td>
<td>Provides information about setting up phones in non-English environments.</td>
</tr>
<tr>
<td>Technical Specifications, on page 219</td>
<td>Provides technical specifications of the Cisco Unified IP Phones.</td>
</tr>
<tr>
<td>Cisco Unified Communications Manager User Addition, on page 224</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 Phones

• Phone Overview, page 1
• Cisco Unified IP Phone 7906G and 7911G, page 2
• Network Protocols, page 3
• Cisco Unified IP Phone 7906 and 7911 Supported Features, page 8
• Cisco Unified IP Phone Security Features, page 10
• Phone Power Consumption, page 21
• Cisco Unified IP Phone Deployment, page 21

Phone Overview

The Cisco Unified IP Phone 7906G and 7911G provides voice communication over an Internet Protocol (IP) network. It functions much like a standard digital business telephone, allowing you to place and receive phone calls and to access features such as mute, hold, transfer, and speed dial. The phone provides additional productivity features because it is connected to the network. These features include access to network information, XML applications, and custom features.

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

Caution

Using 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, refer to the manufacturer documentation of the interfering device.

This chapter includes the following topics:
Cisco Unified IP Phone 7906G and 7911G

The Cisco Unified IP Phone 7906G and 7911G are basic IP phones designed for cubicles, classrooms, factory floors, warehouses, lobbies, and any other location where the phone either complements the user’s set of communication devices or is seldom used. The Cisco Unified IP Phones 7906G and 7911G:

- Provide a graphical display with dynamic softkeys, icons, and scrollable directories for easy access to a core set of business features
- Support up to six calls on one directory number
- Support inline power for both Cisco inline power or IEEE 802.3af Power over Ethernet
- Support enhanced security features including:
  - Manufacturing and field installable certificates
  - Secure Media and Signaling
  - Authenticated Configuration
- Support enhanced calling features plus audio and text XML applications
- Include an integrated 10/100 Mbit Ethernet switch for connecting a PC, preserving the advantage of one cable pull per location (applies to Cisco Unified IP Phones 7911G only)

Buttons and Hardware

You can use the following figures and table to identify the buttons and hardware on your phone.
### Network Protocols

Cisco Unified IP Phones support several industry-standard and Cisco network protocols required for voice communication. The following table provides an overview of the supported network protocols on the Cisco Unified IP Phones 7906G and 7911G.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Phone screen</td>
</tr>
<tr>
<td>2</td>
<td>Cisco Unified IP Phone series</td>
</tr>
<tr>
<td>3</td>
<td>Softkey buttons</td>
</tr>
<tr>
<td>4</td>
<td>Navigation button</td>
</tr>
<tr>
<td>5</td>
<td>Applications Menu button</td>
</tr>
<tr>
<td>6</td>
<td>Hold button</td>
</tr>
<tr>
<td>7</td>
<td>Keypad</td>
</tr>
<tr>
<td>8</td>
<td>Volume button</td>
</tr>
<tr>
<td>9</td>
<td>Handset with light strip</td>
</tr>
<tr>
<td>10</td>
<td>Footstand</td>
</tr>
</tbody>
</table>
Table 1: Supported Network Protocols on the Cisco Unified IP Phones

<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 Phones to</td>
<td>If you use BootP to assign IP addresses to the Cisco Unified IP Phones, the BOOTP Server option shows “Yes” in the network configuration settings on the phone.</td>
</tr>
<tr>
<td></td>
<td>discover startup information such as its IP address.</td>
<td></td>
</tr>
<tr>
<td>Cisco Discovery Protocol (CDP)</td>
<td>CDP is a device-discovery protocol that runs on all Cisco-manufactured</td>
<td>The Cisco Unified IP Phones 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></td>
<td>equipment. A device uses CDP to advertise its existence to other devices</td>
<td></td>
</tr>
<tr>
<td></td>
<td>and receives information about other devices in the network.</td>
<td></td>
</tr>
<tr>
<td>Cisco Peer-to-Peer Distribution</td>
<td>CPPDP is a Cisco proprietary protocol used to form a peer-to-peer</td>
<td>CPPDP is used by the Peer Firmware Sharing feature.</td>
</tr>
<tr>
<td>Protocol (CPPDP)</td>
<td>hierarchy of devices. CPPDP is also used to copy firmware or other files</td>
<td></td>
</tr>
<tr>
<td></td>
<td>from peer devices to neighboring devices.</td>
<td></td>
</tr>
<tr>
<td>Dynamic Host Configuration Protocol</td>
<td>DHCP dynamically allocates and assigns an IP address to network devices.</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 more information about DHCP configurations, see &quot;Dynamic Host Configuration Protocol&quot; and “Cisco TFTP” chapters in the Cisco Unified Communications Manager System Guide.</td>
</tr>
<tr>
<td>(DHCP)</td>
<td>DHCP enables you to connect an IP phone into the network and have the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>phone become operational without your needing to manually assign an IP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>address or to configure additional network parameters.</td>
<td></td>
</tr>
<tr>
<td>HyperText Transfer Protocol (HTTP)</td>
<td>HTTP is the standard way of transferring information and documents</td>
<td>The Cisco Unified IP Phones use HTTP for XML services and troubleshooting purposes.</td>
</tr>
<tr>
<td></td>
<td>across the Internet and the World Wide Web.</td>
<td></td>
</tr>
<tr>
<td>Hypertext Transfer Protocol Secure</td>
<td>Hypertext Transfer Protocol Secure (HTTPS) is a combination of the</td>
<td>Web applications with both HTTP and HTTPS support have two URLs configured. Cisco Unified IP Phones that support HTTPS choose the HTTPS URL.</td>
</tr>
<tr>
<td>(HTTPS)</td>
<td>Hypertext Transfer Protocol with the SSL/TLS protocol to provide</td>
<td></td>
</tr>
<tr>
<td></td>
<td>encryption and secure identification of servers.</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>IEEE 802.1X</td>
<td>The IEEE 802.1X standard defines a client server access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. 802.1X access control allows only Extensible Authentication Protocol over LAN (EAPoL) traffic through a port until a client is authenticated. Traffic can move through a port normally after successful authentication.</td>
<td>The Cisco Unified IP Phones implement the IEEE 802.1X standard by providing support for the following authentication methods: EAP-FAST, EAP-TLS, and EAP-MD5. You should disable the PC port and voice VLAN when 802.1X authentication is enabled. For more information, see 802.1X Authentication, on page 18.</td>
</tr>
<tr>
<td>Internet Protocol (IP)</td>
<td>IP is a messaging protocol that addresses and sends packets across the network.</td>
<td>Network devices must have an IP address, subnet, and gateway assigned to communicate using IP. IP addresses, subnets, and gateways identifications are automatically assigned if you are using the Cisco Unified IP Phones with Dynamic Host Configuration Protocol (DHCP). You must manually assign these properties if you are not using DHCP. The Cisco Unified IP Phones support concurrent IPv4 and IPv6 addresses. Configure the IP addressing mode (IPv4 only, IPv6 only, and both IPv4 and IPv6) in Cisco Unified Communications Manager Administration. For more information, see &quot;Internet Protocol Version 6 (IPv6)&quot; in the Cisco Unified Communications Manager Features and Services Guide.</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 Phones support 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>
</tbody>
</table>
| Link Layer Discovery Protocol-Media Endpoint Devices (LLDP-MED) | LLDP-MED is an extension of the LLDP standard developed for voice products. | The Cisco Unified IP Phones support LLDP-MED on the SW port to communicate information such as:  
  - Voice VLAN configuration  
  - Device discovery  
  - Power management  
  - Inventory management  
| Real-Time Transport Protocol (RTP) | RTP is a standard protocol for transporting real-time data, such as interactive voice and video, over data networks. | Cisco Unified IP Phones use the RTP protocol to send and receive real-time voice traffic from other phones and gateways. |
| Real-Time Control Protocol (RTCP) | RTCP works with RTP to provide QoS data (such as jitter, latency, and round trip delay) on RTP streams. | RTCP is disabled by default. You can enable it on a per phone basis by using Cisco Unified Communications Manager. For more information, see *Network Configuration Menu, on page 82.* |
| Secure Real-Time Transport Protocol (SRTP) | SRTP is available in addition to RTP. SRTP adds security by encrypting media streams during data transport. | For SRTP to work, the phone or phones being called must also support SRTP or else those phones cannot decrypt the secure media stream. |
| Session Initiation Protocol (SIP) | SIP is the Internet Engineering Task Force (IETF) standard for multimedia conferencing over IP. SIP is an ASCII-based application-layer control protocol (defined in RFC 3261) that can be used to establish, maintain, and terminate calls between two or more endpoints. | SIP is designed to address the functions of signaling and session management within a packet telephony network. Signaling allows call information to be carried across network boundaries. Session management provides the ability to control the attributes of an end-to-end call.  
You can configure the Cisco Unified IP Phones to use either SIP or Skinny Client Control Protocol (SCCP). Cisco Unified IP Phones do not support the SIP protocol when the phones are operating in IPv6 address mode. |
### 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 are supported by all endpoints in the conference.</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 these parameters to be configured 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 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 when securely registering with Cisco Unified Communications Manager. For more information, refer to 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.</td>
<td>TFTP requires a TFTP server in your network, which can be automatically identified from the DHCP server. If more than one TFTP server is running in your network, you must manually assign a TFTP server to each phone locally. For more information, see &quot;Cisco TFTP&quot; 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 receive and process UDP messages.</td>
</tr>
</tbody>
</table>

### Related Topics

- Cisco Unified Communications Product Interactions, on page 27
- Phone Startup Process, on page 32
- Network Configuration Menu, on page 57
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 7906 and 7911 Supported Features

Cisco Unified IP Phones 7906G and 7911G function much like traditional analog phones, allowing you to place and receive phone calls. In addition to traditional telephony features, each Cisco Unified IP Phone includes features that enable you to administer and monitor the phone as a network device.

Feature Overview

Cisco Unified IP Phones provide core business features 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.

You must configure Cisco Unified IP Phones to prepare them to access Cisco Unified Communications Manager and the rest of the IP network. There are fewer settings to configure when DHCP is used in the network. Phones do provide for the manual configuration of IP address, TFTP server, and subnet information.

Cisco Unified IP Phones can interact with other services and devices on your IP network to provide enhanced functionality. For example, you can integrate Cisco Unified Communications Manager with the corporate Lightweight Directory Access Protocol 3 (LDAP3) standard directory to enable users to search for coworkers.
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 Phones area network device, you can obtain detailed status information from it directly. This information can assist you with troubleshooting any problems users might encounter when using their Cisco Unified IP phones.

Related Topics
- Services Setup, on page 124
- Corporate and Personal Directory Setup, on page 119
- Model Information, Status, and Statistics, on page 143
- Cisco Unified IP Phone Settings, on page 53
- Features, Templates, Services, and Users, on page 97
- Troubleshooting and Maintenance, on page 179

### Telephony Feature Administration

You can modify certain settings for the Cisco Unified IP Phones from the Cisco Unified Communications Manager Administration application. Use this web-based application to set up phone registration criteria and calling search spaces, to configure corporate directories and services, and to modify phone button templates, among other tasks. For more information, see *Cisco Unified Communications Manager Administration Guide*.

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

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


You can access Cisco Unified Communications Manager Business Edition 5000 documentation at this location:


Related Topics
- Telephony Features Available for Cisco Unified IP Phone, on page 98

### 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 call or firmware versions on the phone.

Related Topics
- Cisco Unified IP Phone Settings, on page 53
- Model Information, Status, and Statistics, on page 143

### 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 view and order various user guides, including wallet cards.

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

Related Topics

Internal Support Web Site, on page 203

Cisco Unified IP Phone Security Features

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

To alleviate these threats, the Cisco Unified Communications 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 between Cisco Unified IP Phones.

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 more information, see "Configuring Encrypted Phone Configuration Files" in Cisco Unified Communications Manager Security Guide.

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

Table 2: Cisco Unified IP Phone security topics

<table>
<thead>
<tr>
<th>Topic</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detailed explanation of security, including set up, configuration, and troubleshooting information for Cisco Unified Communications Manager and Cisco Unified IP Phones</td>
<td>See Troubleshooting Guide for Cisco Unified Communications Manager.</td>
</tr>
<tr>
<td>Identifying phone calls for which security is implemented</td>
<td>See Authenticated, Encrypted, and Protected Phone Calls, on page 14.</td>
</tr>
<tr>
<td>Transport Layer Security (TLS) connection</td>
<td>• See Network Protocols, on page 3&lt;br&gt;• See Phone Configuration Files, on page 3</td>
</tr>
<tr>
<td>Topic</td>
<td>Reference</td>
</tr>
<tr>
<td>-------</td>
<td>-----------</td>
</tr>
</tbody>
</table>
| 802.1X authentication for Cisco Unified IP Phones | See these sections:  
  - 802.1X Authentication, on page 18  
  - Security Configuration Menu, on page 89  
  - 802.1X Authentication and Status, on page 94  
  - Cisco Unified IP Phone Security Problems, on page 186 |
| Security and the phone startup process | See Phone Startup Process, on page 32. |
| Security and phone configuration files | See Phone Configuration Files, on page 31. |
| Changing the TFTP Server 1 or TFTP Server 2 option on the phone when security is implemented | See Network Configuration Menu, on page 57. |
| Understanding security icons in the Communications Manager 1 through Communications Manager 5 options in the Device Configuration Menu on the phone | See Unified CM Configuration Menu, on page 69. |
| Items on the Security Configuration menu that you access from the Device Configuration menu on the phone | See Security Configuration Menu, on page 80. |
| Items on the Security Configuration menu that you access from the Settings menu on the phone | See Security Configuration Menu, on page 89. |
| Unlocking the Certificate Trust List (CTL) and Identity Trust List (ITL) files | See Unlock CTL and ITL Files, on page 91. |
| Disabling access to a phone’s web pages | See Control Web Page Access, on page 165. |
| Deleting the CTL and ITL files from the phone | See Cisco Unified IP Phone Reset or Restore, on page 197. |
| Resetting or restoring the phone | See Cisco Unified IP Phone Reset or Restore, on page 197. |
| Extension Mobility HTTPS Support | See Network Protocols, on page 3. |
| 802.1X Authentication for Cisco Unified IP Phones | See these sections:  
  - 802.1X Authentication, on page 18  
  - 802.1X Authentication and Status, on page 94  
  - Cisco Unified IP Phone Security Problems, on page 186  
  - Trust List Menu, on page 93 |
Supported Security Features

This section provides an overview of the security features that the phone supports. For more information about these features and about Cisco Unified Communications Manager and Cisco Unified IP Phone security, see Cisco Unified Communications Manager Security Guide.

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

Most security features are available only if a CTL or ITL file or both are installed on the phone. For more information about the CTL and ITL files, see the Cisco Unified Communications Manager Security Guide.

Table 3: 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 is loaded on a phone. Tampering with the image causes a phone to fail the authentication process and reject the new image.</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. See 802.1X Authentication, on page 18 for more information.</td>
</tr>
<tr>
<td>Customer-site certificate installation</td>
<td>Each Cisco Unified IP Phone requires a unique certificate for device authentication. Phones include a manufacturing installed certificate (MIC), but for additional security, you can specify in Cisco Unified Communications Manager Administration that a certificate be installed by using the Certificate Authority Proxy Function (CAPF). Alternatively, you can install an Locally Significant Certificate (LSC) from the Security Configuration menu on the phone. See Cisco Unified IP Phone Security, on page 51 for more information.</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 by using transport layer security (TLS) protocol. Cisco Unified Communications Manager does not register phones configured in authenticated or encrypted mode unless they can be authenticated by the Cisco Unified Communications Manager.</td>
</tr>
</tbody>
</table>
### Supported Security Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 the 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>Manufacturing installed certificate</td>
<td>Each Cisco Unified IP Phone 7906G and 7911G contains a unique 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 a 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 SRTP to ensure that the media streams between supported devices proves secure and that only the intended device receives and reads the data. Includes creating a media master key pair for the devices, delivering the keys to the devices, and securing the delivery of the keys 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>Optional disabling of the web server</td>
<td>You can prevent access to the web page for a phone, which displays a variety of operational statistics for the phone.</td>
</tr>
</tbody>
</table>
Additional security options, which you control from Cisco Unified Communications Manager Administration include:

- Disable PC port (applies to 7911G only)
- Disable Gratuitous Address Resolution Protocol (GARP)
- Disable PC Voice VLAN access (applies to 7911G only)
- Disable access to the Setting menus, or provide restricted access that allows access to the User Preferences menu and saving volume changes only
- Disable access to web pages for a phone

You can view current settings for the PC Port Disabled, GARP Enabled, and Voice VLAN enabled options by looking at the phone Security Configuration menu.

**Related Topics**
- Authenticated, Encrypted, and Protected Phone Calls, on page 14
- 802.1X Authentication, on page 18
- Security Restrictions, on page 20
- Device Configuration Menu, on page 69

### Security Profiles

All Cisco Unified IP Phones that support Cisco Unified Communications Manager 5.0 and later use a security profile, which defines whether the phone is nonsecure, authenticated, or encrypted. For information about configuring the security profile and applying the profile to the phone, see the *Cisco Unified Communications Manager Security Guide*.

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

**Related Topics**
- Authenticated, Encrypted, and Protected Phone Calls, on page 14
- Security Restrictions, on page 20
- Security Configuration Menu, on page 80

### 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 LCD screen on the phone. You can also determine if the connected phone is secure and protected if a security tone plays at the beginning of the call.
In an authenticated call, all devices participating in the establishment of the call are trusted devices, and authenticated by Cisco Unified Communications Manager. When a call is setting up, the call is authenticated end-to-end. The call progress icon to the right of the call duration timer in the phone LCD screen changes to the following icon:

In an encrypted call, all devices participating in the establishment of the call are trusted devices, and authenticated by the Cisco Unified Communications Manager. In addition, call signaling and media streams are encrypted. An encrypted call offers a high level of security, providing integrity and privacy to the call. When a call in progress is being encrypted, the call progress icon to the right of the call duration timer in the phone LCD screen changes to the following icon:

---

**Note**

If the call is routed through a non-IP call leg, for example, PSTN, the call will be nonsecure even though it is encrypted within the IP network and has a lock icon associated with it.

A security tone plays at the beginning of a protected call to indicate that the other connected phone is also receiving and transmitting encrypted audio and possible video. If your call is connected to a nonprotected 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 10
- [802.1X Authentication](#), on page 18
- [Security Restrictions](#), on page 20

---

**Secure Conference Call Identification**

You can initiate a secure conference call and monitor the security level of participants. A secure conference call is established using 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.
There are interactions, restrictions, and limitations that affect the security level of the conference call depending on the security mode of the participant’s phones and the availability of secure conference bridges. See Call Security Interactions and Restrictions, on page 16 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.

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

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>
<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>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 5: 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>Secure (encrypted)</td>
<td>Join</td>
<td>Encrypted or authenticated</td>
<td>Secure conference bridge Conference remains secure (encrypted or authenticated)</td>
</tr>
<tr>
<td>Nonsecure</td>
<td>cBarge</td>
<td>All participants are encrypted</td>
<td>Secure conference bridge Conference changes to nonsecure</td>
</tr>
</tbody>
</table>

Cisco Unified IP Phone 7906G and 7911G Administration Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)
### 802.1X Authentication

This section provides 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.

<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>Meet-Me</td>
<td>Minimum security level is encrypted</td>
<td>Initiator receives message Does not meet Security Level, call rejected.</td>
</tr>
<tr>
<td>Secure (encrypted)</td>
<td>Meet-Me</td>
<td>Minimum security level is authenticated</td>
<td>Secure conference bridge Conference accepts encrypted and authenticated calls</td>
</tr>
<tr>
<td>Secure (encrypted)</td>
<td>Meet-Me</td>
<td>Minimum security level is nonsecure</td>
<td>Only secure conference bridge available and used Conference accepts all calls</td>
</tr>
</tbody>
</table>
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 Practices, 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 enabling it 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 (including Cisco Catalyst switches) support multidomain authentication. The switch configuration determines whether you can connect a PC to the phone PC port.

  - **Enabled**—If you are using a switch that supports multidomain authentication, you can enable the PC port and connect a PC to it. In this case, Cisco 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: [http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html](http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html)

  - **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 both the phone and the PC.

- **Configure Voice VLAN**—Because the 802.1X standard does not account for VLANs, you should configure this setting based on the switch support.

  - **Enabled**—If you are using a switch that supports multidomain authentication, you can continue to use the voice VLAN.

  - **Disabled**—If the switch does not support multidomain authentication, disable the Voice VLAN and consider assigning the port to the native VLAN.

- **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.

### Related Topics

- Security Configuration Menu, on page 80
- 802.1X Authentication and Status, on page 94
UCR 2008

The IP Phones using SCCP support Unified Capabilities Requirements (UCR) 2008 by providing the following functions:

- Support for Federal Information Processsing Standard (FIPS) 104-2—To support FIPS 104-2, the phone requires:
  - The use of Power On Self Testing (POST) to ensure that the appropriate encryption algorithms are available. If the phone does not have the correct modules in the firmware, the phone fails to boot.
  - The use of HTTPS for all internet communications.
  - The disabling of Web Access to the phone.
  - That the CUCM to be set up for FIPS compliance (for example, disabling 802.1x EAP-MD5).

- TVS IPv6—The phone displays the IPv6 address of a Trust Verification Service (TVS) server, if an IPv6 address is available.

- 80-bit SRTCPTagging—The phone handles both 32-bit and 80-bit SRTCP packet headers seamlessly.

Some of these functions require the configuration of specific parameters in Cisco Unified Communications Manager.

The following table shows where you can find addition information about UCR 2008 in this and other documents.

<table>
<thead>
<tr>
<th>Topic</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detailed explanation of security, including set up, 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>Setting up UCR 2008 parameters</td>
<td>See UCR 2008 Setup, on page 130.</td>
</tr>
<tr>
<td>Troubleshooting POST problems</td>
<td>See Cisco Unified IP Phone Displays Security Error Message, on page 183.</td>
</tr>
</tbody>
</table>

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

When deploying a new Unified Communications system, system administrators and network administrators must complete several initial configuration tasks to prepare the network for Unified Communications service. For information and a checklist for setting up and configuring a complete Cisco Unified Communications network, see “System Configuration Overview” in the *Cisco Unified Communications Manager System Guide*.

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

## 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 configuring phones in Cisco Unified Communications Manager, see the following documentation:

- “Cisco Unified IP Phone” chapter, *Cisco Unified Communications Manager System Guide*
- “Configuring Cisco Unified IP Phone Configuration” chapter, *Cisco Unified Communications Manager Administration Guide*
- “Autoregistration” chapter, *Cisco Unified Communications Manager Administration Guide*
Set Up Cisco Unified IP Phones 7906G and 7911G in Cisco Unified Communications Manager

The following steps provide an overview and checklist of configuration tasks for the Cisco Unified IP Phones 7906G and 7911G in Cisco Unified Communications Manager. The steps present tasks in 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:

• Phone Model
• MAC address
• Physical location of the phone
• Name or user ID of phone user
• Device pool
• Calling search space and location information (if used)
• Number of lines, associated directory numbers (DNs), and partitions to assign to the phone
• Cisco Unified Communications Manager user to associate with the phone
• Phone usage information that affects phone button template, softkey template, phone features, IP Phone services, or phone applications

The information provides list of configuration requirements for setting up phones and identifies preliminary configuration that you need to perform before configuring individual phones, such as phone button templates or softkey templates.

For more information, see "Cisco Unified IP Phone" chapter in Cisco Unified Communications Manager System Guide, and Telephony Features Available for Cisco Unified IP Phone, on page 98.

Step 2 Customize phone button templates (if required). This adds the Privacy feature to meet user needs.

For more information, see "Phone Button Template Configuration" chapter in Cisco Unified Communications Manager Administration Guide, and Phone Button Templates, on page 120.

Step 3 Add and configure the phone by completing these required fields in the Phone Configuration window:

• Phone type
• MAC address
• Device pool
• Button template
• Product Specific Configuration
• Softkey template (if customized)
Add the device with its default settings to the Cisco Unified Communications Manager database.

For more information, see "Cisco Unified IP Phone Configuration" chapter in Cisco Unified Communications Manager Administration Guide.

For information about Product Specific Configuration fields, see ? Button Help in the Phone Configuration window.

**Note** If you want to add both the phone and user to the Cisco Unified Communications Manager database at the same time, see "User/Phone Configurations" in Cisco Unified Communications Manager Administration Guide.

**Step 4** Add and configure the directory number on the phone by completing these required fields in the Directory Number Configuration window.

- Directory number
- Multiple Calls and Call Waiting
- Call Forwarding and Pickup (if used)
- Voice Messaging (if used)

Adds primary and secondary directory numbers and features associated with directory numbers to the phone. For more information, see "Directory Number Configuration" chapter in Cisco Unified Communications Manager Administration Guide and Telephony Features Available for Cisco Unified IP Phone, on page 98.

**Step 5** Customize softkey templates (optional). Adds, deletes, or changes order of softkey features that display on the user's phone to meet feature usage needs.

For more information, see "Softkey Template Configuration" chapter in Cisco Unified Communications Manager Administration Guide, and Softkey Templates, on page 123.

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

**Note** Users can change speed-dial settings on their phones with Cisco Unified Communications Manager User Options.

For more information, see the Cisco Unified Communications Manager Administration Guide, "Cisco Unified IP Phone Configuration" chapter, "Configuring Speed-Dial Buttons" section.

**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.

For more information, see "Cisco Unified IP Phone Services Configuration" chapter in Cisco Unified Communications Manager Administration Guide, and Services Setup, on page 124.

**Step 8** Assign services to phone buttons (optional). Provides single button access to an IP phone service or URL. For more information, see Cisco Unified Communications Manager Administration Guide, "Cisco Unified IP Phone Configuration" chapter, "Adding a Cisco Unified IP Phone Service to a Phone Button" section.

**Step 9** Add user information by configuring required fields (optional).

- Name (last)
- User ID
- Password (for User Options web pages)
- PIN (for use with Extension Mobility
Adds user information to the global directory for Cisco Unified Communications Manager.

**Note**  
To search for a user in the Corporate Directory, you must add users to Cisco Unified Communications Manager.

For more information, see “End User Configuration” chapter in *Cisco Unified Communications Manager Administration Guide* and *Cisco Unified Communications Manager User Addition*, on page 124.

**Note**  
If your company uses a Lightweight Directory Access Protocol (LDAP) directory to store information on users, you install and configure Cisco Unified Communications to use your existing LDAP directory, see *Corporate and Personal Directory Setup*, on page 119.

**Note**  
If you want to add both the phone and user to the Cisco Unified Communications Manager database at the same time, see "User/Phone Configurations" chapter in *Cisco Unified Communications Manager Administration Guide*.

**Step 10**  
Add 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. For example, you must add users to the Standard Cisco CCM End Users group so users can access Cisco Unified Communications Manager User Options.

For more information, see Cisco Unified Communications Manager Administration Guide, "User Group Configuration” chapter, “Adding Users to a User Group” section.

**Step 11**  
Associate a user with a phone (optional).
Provides users with control over their phone such as forwarding calls or adding speed-dial numbers or services.

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

For more information, see *Cisco Unified Communications Manager Administration Guide*, "End User Configuration” chapter, “Associating Devices to a User” section.

---

### 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 Phones 7906G and 7911G

The following steps provide an overview and checklist of installation tasks for the Cisco Unified IP Phone 7906G and 7911G. The steps present tasks in a suggested order to guide you through the phone installation process. Some tasks are optional, depending on your system and user needs. For detailed procedures and information, refer to the sources in the steps.

Procedure

Step 1  Choose the power source for the phone:

- Power over Ethernet (PoE)
- External power supply

Determines how the phone receives power. For more information, see Cisco Unified IP Phone Power, on page 29

Step 2  Assemble the phone, adjust phone placement, and connect the network cable.
Locates and installs the phone in the network. For more information, see Install Cisco Unified IP Phones, on page 44.

Step 3  Monitor the phone startup process.
Verifies that phone is configured properly. For more information, see Phone Startup Verification, on page 50.

Step 4  If you are using DHCP to configure the network settings on the phone, 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:

- 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 with the network administrator if you need to assign an alternative TFTP server instead of using the TFTP server assigned by DHCP.

Step 5  If you are not using DHCP to configure the network settings on the phone, you must configure the IP address, subnet mask, TFTP server, and default router locally on the phone, choose Settings > Network Configuration > IPv4 Configuration:
To disable DHCP and manually set an IP address:
a) To disable DHCP, 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.

Note Choose Settings > Network Configuration and enter the domain name where the phone resides.

For more information, see Network Settings, on page 50 and Network Configuration Menu, on page 57.

Step 6  Set up security on the phone.
Provides protection against data tampering threats and identity theft of phones. For more information, see Cisco Unified IP Phone Security, on page 51

**Step 7** Make calls with the Cisco Unified IP Phones.
Verifies that the phone and features work correctly. For more information, see the Cisco Unified IP Phones 7906G and 7911G User Guide for Cisco Unified Communications Manager (SCCP and SIP).

**Step 8** Provide information to users about how to use their phones and how to configure their phone options.
Ensures that users have adequate information to successfully use their Cisco Unified IP Phones. For more information, see Internal Support Web Site, on page 203
Cisco Unified IP Phones and Telephony Networks

- Phone and Telephony Network Overview, page 27
- Cisco Unified Communications Product Interactions, page 27
- Cisco Unified IP Phone Power, page 29
- Phone Configuration Files, page 31
- Phone Startup Process, page 32
- Cisco Unified Communications Manager Phone Addition Methods, page 33
- Cisco Unified IP Phones and Different Protocols, page 36
- Cisco Unified IP Phone MAC Address Determination, page 37

Phone and Telephony Network Overview

Cisco Unified IP Phones enable you to communicate by using voice over a data network. Cisco Unified IP Phones depend on several key Cisco Unified Communications and network components. These include Cisco Unified Communications Manager, DNS servers, DHCP servers, TFTP servers, and media resources.

This chapter provides an overview of the interaction between the Cisco Unified IP Phones 7906G and 7911G and other key components of the Voice over IP (VoIP) network and focuses on the interactions between the Cisco Unified IP Phones 7906G and 7911G and Cisco Unified Communications Manager, TFTP server, and switches.

Cisco Unified Communications Product Interactions

Cisco Unified IP Phones must be connected to a networking device (such as a Catalyst switch) to function in the Unified Communications network. You must also register the Cisco Unified IP Phone with a Cisco Unified Communications Manager system before sending and receiving calls.
Cisco Unified IP Phone and Cisco Unified Communications Manager Interaction

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, integrating traditional PBX functionality with the corporate IP network. Cisco Unified Communications Manager manages the components of the Cisco Unified Communications 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 authentication and encryption if configured for the communications system.

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

For an overview of security functionality for the Cisco Unified IP Phones, see Supported Security Features, on page 12.

Note

If the Cisco Unified IP Phones 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

Telephony Features Available for Cisco Unified IP Phone, on page 98

Cisco Unified IP Phones and VLAN Interaction

The Cisco Unified IP Phones 7911G has an internal Ethernet switch. The switch enables forwarding of packets to the phone and to the network port and access port on the back of the phone. The Cisco Unified IP Phones 7906G has an Ethernet port. This port enables forwarding of packets to the phone and to the network port.

If a computer is connected to the access port on a Cisco Unified IP Phones 7911G, the computer and the phone share the same physical link to the switch and the same port on the switch. This shared physical link affects the VLAN configuration on the network in the following ways:

• Although current VLANs might be configured on an IP subnet basis, additional IP addresses may not be available to assign the phone to the same subnet as other devices that connect to the same port.

• Data traffic present on the data/native VLAN may reduce the quality of VoIP traffic.

• Network security may necessitate the isolation of the VLAN voice traffic from the VLAN data traffic.

You can resolve these issues by isolating the voice traffic onto a separate VLAN, so that the switch port to which the phone is connected uses separate VLANs for the following types of traffic:

• 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 connected to the switch through the access port of the IP phone (native VLAN, Cisco Unified IP Phone 7911G only)
Isolating 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 in which there are not enough IP addresses for each phone.

**Note**

Do not configure the switch port for VLAN 1 due to a limitation with the Cisco Unified IP Phone 7911. When the switch port is configured to VLAN 1, the phone forwards tagged packets in VLAN 1 to the switch.

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


**Related Topics**

- Phone Startup Process, on page 32
- Network Configuration Menu, on page 57

**Cisco Unified IP Phone Power**

The Cisco Unified IP Phones 7906G and 7911G can be powered with external power or with Power over Ethernet (PoE). External power is provided through a separate power supply. PoE is provided by a switch through the Ethernet cable attached to a phone.

**Power Guidelines**

The following table provides guidelines that apply to external power and to PoE power for the Cisco Unified IP Phone 7906G and 7911G.

**Table 7: Guidelines for Cisco Unified IP Phone 7906G and 7911G Power**

<table>
<thead>
<tr>
<th>Power type</th>
<th>Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>External power—Provided through a Cisco external power supply.</td>
<td>The Cisco Unified IP Phone Series 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 Phones Power Injector may be used with any Cisco Unified IP Phones. Functioning as a midspan device, the injector delivers inline power to the attached phone. The Cisco Unified IP Phones Power Injector is connected between a switch port and the Cisco Unified IP Phones, and supports a maximum cable length of 100 m between the unpowered switch and the phone.</td>
</tr>
</tbody>
</table>
Power type | Guidelines
--- | ---
PoE power—Provided by a switch through the Ethernet cable attached to the phone. | • The Cisco Unified IP Phones 7906G and 7911G support both Cisco inline power and IEEE 802.3af Power over Ethernet.
• 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 running on your switch supports your intended phone deployment. Refer to the documentation for your switch for operating system version information.

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

For related information about power, refer to the documents shown in the following table. These documents provide information about these topics:

- Cisco switches that work with the Cisco Unified IP Phones
- The Cisco IOS releases that support bidirectional power negotiation
- Other requirements and restrictions regarding power

<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 parameters for connecting to Cisco Unified Communications Manager. In general, any time you make a change in Cisco Unified Communications Manager that requires the phone to be reset, a change is automatically made to the configuration file for the phone.

Configuration files also contain information about which image load the phone should be running. If this image load differs from the one currently loaded on a phone, 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 Administration. Otherwise, the phone establishes a TCP connection.

Note
Cisco Extension Mobility Cross Cluster is an exception. 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 detailed information, see "Configuring Encrypted Phone Configuration Files" in Cisco Unified Communications Manager Security Guide.

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 containing a certificate assigned to the Cisco Unified Communications Manager and TFTP.

If auto registration is not enabled and you did not add the phone to the Cisco Unified Communications Manager database, the phone does not attempt to register with Cisco Unified Communications Manager. The phone continually displays the Configuring IP message until you either enable autoregistration or add the phone to the Cisco Unified Communications Manager database.

If the phone has registered before, the phone accesses the configuration file named SEPmac_address.cnf.xml, where mac_address is the MAC address of the phone. For more information about how the phone interacts with the TFTP server, see the Cisco Unified Communications Manager System Guide, "Cisco TFTP" section.

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 "Configuring Encrypted Phone Configuration Files" in Cisco Unified Communications Manager Security Guide.

SIP Dial Rules

For Cisco Unified IP Phones running under SIP, the administrator uses dial rules to configure SIP phone dial plans. These dial plans must be associated with a SIP phone device to enable dial plans to be sent to the configuration file. If the administrator does not configure a SIP phone dial plan, the phone does not display
any indication of a dial plan. In this case, you must press the Dial softkey, unless the phone supports key press markup language (KPML).

For more information on configuring SIP dial rules, see the *Cisco Unified Communications Manager Administration Guide*.

## Phone Startup Process

Cisco Unified IP Phones go through a standard startup process when connecting to the VoIP network. The following steps describe this process. Depending on your specific network configuration, not all steps may occur on your Cisco Unified IP Phone.

### Procedure

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

For more information, see *Cisco Unified IP Phone Power*, on page 29 and *Startup Problems*, on page 179.

**Step 2** The Cisco 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. Using this image, the phone initializes its software and hardware.

For more information, see *Startup Problems*, on page 179.

**Step 3** Configuring VLAN.
If the Cisco IP Phone is connected to a Cisco switch, the switch 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.

If a third-party switch is used and VLANs are configured, the VLAN on the phone must be manually configured.

For more information, see *Network Configuration Menu*, on page 57 and *Startup Problems*, on page 179.

**Step 4** Obtaining an IP Address.
If the Cisco IP Phone is using DHCP to obtain an IP address, the phone queries the DHCP server to obtain one. If your network does not use DHCP, you must assign static IP addresses to each phone locally.

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 assigned by DHCP.

For more information, see *Network Configuration Menu*, on page 57 and *Startup Problems*, on page 179.

**Step 5** Accessing a TFTP Server.
For more information, see *Network Configuration Menu*, on page 57 and *Startup Problems*, on page 179.

**Step 6** Requesting the CTL file.
The TFTP server stores the CTL file. This file contains the certificates necessary for establishing 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 Requesting the ITL file

The phone requests the ITL file after it requests the CTL file. The ITL file contains the certificates of the entities that the phone can trust. The certificates are used for authenticating a secure connection with the servers or to authenticating a digital signature signed by the servers.


Cisco Unified Communications Manager Phone Addition Methods

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

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

Table 8: Methods for adding phones to the Cisco Unified Communications Manager database

<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>
<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>Using the Cisco Unified Communications Manager Administration</td>
<td>Yes</td>
<td>Requires phones to be added individually</td>
</tr>
<tr>
<td>Using BAT</td>
<td>Yes</td>
<td>Can add groups of same model of phone.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Can schedule when phones are added to the Cisco Unified Communications Manager database.</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.

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 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 to *Cisco Unified Communications Manager System Guide*.

### Related Topics

- Cisco Unified IP Phone MAC Address Determination, on page 37

## Add Phones with BAT

Cisco Unified Communications Manager Bulk Administration Tool (BAT) enables you to perform batch operations, which includes registration, on multiple phones. To access BAT, choose the **Bulk Administration** drop-down menu in Cisco Unified Communications Manager Administration,

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 the Cisco Unified Communications Manager, perform these steps:

### Procedure

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

---

Cisco Unified IP Phone 7906G and 7911G Administration Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)
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

Step 1  Take one of these actions:

- To autoregister the phone, set the Auto Registration Phone Protocol enterprise parameter in Cisco Unified Communications Manager Administration to SIP.
- To provision the phone by using the Bulk Administration Tool (BAT), choose the appropriate phone model and choose SIP from BAT.
- To provision the phone manually, make the appropriate changes for SIP on the Phone Configuration window in Cisco Unified Communications Manager Administration.

See the Cisco Unified Communications Manager Administration Guide for more information about Cisco Unified Communications Manager configuration. See Bulk Administration Tool Administration Guide for more information about using BAT.

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

Step 3  Save the configuration updates, click Apply Config, click OK in the Apply Configuration Information window, and have the user power cycle the phone.

Related Topics

Network Settings, on page 50

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

Cisco Unified IP Phone MAC Address Determination

Several of the procedures that are described 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, press the Applications Menu button, then choose Settings > Network Configuration, and look at the MAC Address field.
- Look at the MAC label on the back of the phone.
- Display the web page for the phone and click the Device Information hyperlink.

For more information, see Access Web Page for Phone, on page 164.
Cisco Unified IP Phone Installation

- Phone Installation Overview, page 39
- Before You Begin, page 39
- Cisco Unified IP Phones 7906G and 7911G Components, page 40
- Install Cisco Unified IP Phones, page 44
- Mount Phone on Wall, page 49
- Phone Startup Verification, page 50
- Network Settings, page 50
- Cisco Unified IP Phone Security, page 51

Phone Installation Overview

This chapter helps you install the Cisco Unified IP Phones 7906G and 7911G on a Cisco Unified Communications 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 its functionality. For more information, see Cisco Unified IP Phones and Telephony Networks, on page 27.

Before You Begin

Before installing the Cisco Unified IP Phone, review the requirements in this section.

Network Requirements

For the Cisco Unified IP Phone 7906G and 7911G to successfully operate as a Cisco Unified IP Phone endpoint in your network, your network must meet these requirements:
• Working Voice over IP (VoIP) Network
  
  ° VoIP configured on your Cisco routers and gateways
  
  ° Cisco Unified Communications Manager Release 4.x or higher installed in your network and configured to handle call processing

  Note  
  The minimum firmware release that must be installed on the phone is 7.2(1).

• 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. If the Cisco Unified Communications Manager server is located in a different time zone than the phones, the phones will not display the correct local time.

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 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 Administration before connecting 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 Administration to configure and assign features to the Cisco Unified IP Phones.

In Cisco Unified Communications Manager Administration, you can add users to the database and associate them with specific phones. In this way, users can access their Cisco Unified CM User Option page to configure items such as Call Forward, Speed Dial, and voice message system options.

Related Topics
  
  Cisco Unified Communications Manager Phone Addition Methods, on page 33
  Telephony Features Available for Cisco Unified IP Phone, on page 98
  Cisco Unified Communications Manager User Addition, on page 124

Cisco Unified IP Phones 7906G and 7911G Components

The Cisco Unified IP Phones 7906G and 7911G include these components on the phone or as accessories for the phone:
Network and Access Ports

The following ports are available on the Cisco Unified IP Phones 7906G and 7911G:

- **Network port**—Labeled 10/100 SW. Use the 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 the Cisco Catalyst switch over this connection. See [Cisco Unified IP Phone Power](#) on page 29 for details.

- **Access port** (Cisco Unified IP Phone 7911G only)—Labeled 10/100 PC. Use the access port to connect a network device, such as a computer, to the phone. You must use a straight-through cable on this port.

Each port supports 10/100 Mbps half- or full-duplex connections to external devices. The speed and connection type are set through auto-negotiation. You can use either Category 3 or 5 cabling for 10-Mbps connections, but you must use Category 5 for 100 Mbps connections.

See [Cisco Unified IP Phone 7906G Installation](#) on page 47 and [Cisco Unified IP Phone 7911G Installation](#) on page 48 for the connection ports available on the back of the Cisco Unified IP Phone 7906G and 7911G.

Handset

The Cisco Unified IP Phone uses a handset that is designed especially for the phone. The handset includes a light strip to indicate incoming calls and voice messages waiting.

To connect a handset to the Cisco Unified IP Phone, plug the cable into the handset and into the Handset port on the back of the phone.

Speaker

The Cisco Unified IP Phone 7906G and 7911G include a speaker that you can use to monitor calls. You can enable either the Monitor mode or Group Listen mode to allow users to listen on the speaker.

The speaker is enabled by default. You can disable the speaker using Cisco Unified Communications Manager Administration.

**Disable Speakerphone**

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

**Procedure**

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

Users can only listen to a call on the speaker in Monitor mode. To speak to the other party on the call, users must pick up the handset.

Monitor mode is enabled by default if the speaker is enabled on Cisco Unified Communications Manager Administration.

From the phone, users can turn on the Monitor function with the Monitor softkey, and turn off this function with the MonOff softkey or by picking up the handset.

Group Listen Mode

The handset and speaker can be active simultaneously in Group Listen mode. One user speaks into the handset with others can listen on the speaker.

Set Up Group Listen Mode on Cisco Unified Communications Manager

Group Listen mode is disabled by default.

The Monitor feature softkeys are not available if Group Listen mode is enabled.

To enable this mode, you use the Phone Configuration window in Cisco Unified Communications Manager Administration.

Procedure

Step 1
From Cisco Unified Communications Manager Administration, choose Device > Phone and locate the phone you want to modify.

Step 2
In the Phone Configuration window for the phone (Product Specific Configuration section), check the Enable Group Listen check box.

Group Listen Activation on Phone

Group Listen softkeys are displayed if Group Listen mode is enabled on Cisco Unified Communications Manager. However, these softkeys cannot be configured using the Cisco Unified Communications Manager softkey template.

- **GL**Listen: Activates Group Listen on the phone. Displayed when Group Listen mode is enabled but not activated on the phone. After Group Listen is activated on the phone (by pressing **GL**isten), users can deactivate it by hanging up the handset or by pressing **GLO**ff.

- **GLO**ff: Deactivates Group Listen on the phone. Displayed when Group Listen mode is enabled and activated on the phone.
The GListen and GLOff softkeys replace the Monitor and MonOff softkeys when Group Listen mode is enabled in Cisco Unified Communications Manager.

**Headset**

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

Cisco recommends 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 cell 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. Humming or buzzing sounds can be caused by a range of outside sources; for example, electric lights, electric motors, or large PC monitors. See External Device Use, on page 44 for more information.

**Note**

In some cases, hum may be reduced or eliminated by using a local power cube or power injector.

These environmental and hardware inconsistencies in the locations where Cisco Unified IP Phones are deployed means that there is not a single headset solution that is optimal for all environments.

Cisco recommends that customers test headsets in their intended environment to determine performance before making a purchasing decision and deploying in mass quantities.

**Note**

The Cisco Unified IP Phone 7906G and 7911G supports wideband headsets.

**Audio Quality**

Beyond physical, mechanical, and technical performance, the audio portion of a headset must sound good to the user and to the party on the far end. Sound quality is subjective and Cisco cannot guarantee the performance of any headsets. However, a variety of headsets from leading headset manufacturers are 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.

**Headset Connection**

To connect a headset to the Cisco Unified IP Phones, plug it into the RJ-9 Handset port on the back of the phone. Depending on headset manufacturer's recommendations, an external amplifier may be required. See headset manufacturer's product documentation for details.

You can use the headset with all of the features on the Cisco Unified IP Phones, including using the Volume button.
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 Phones

You must connect the Cisco Unified IP Phones to the network and to a power source before using it.

Note

Always upgrade the phone to the current firmware image before installation.

Note

Before using external devices, read External Device Use, on page 44 for safety and performance information.

To install a Cisco Unified IP Phones, perform the following tasks.

Procedure

Step 1  Connect the footstand to the back of the phone. See Footstand Installation, on page 46.
Step 2  Connect the handset to the Handset port.
Step 3  Connect the power supply to the Cisco DC Adapter port (DC48V).

(Optional) When connecting phones powered by an external power supply, you must connect the power supply to the phone before connecting the Ethernet cable to the phone.

When disconnecting the phone, you must disconnect the Ethernet cable before disconnecting the power supply.
**Step 4**  
Connect a Category 3 or 5 straight-through Ethernet cable from the switch to the 10/100 SW port. Each Cisco Unified IP Phone ships with one Ethernet cable in the box.

**Step 5**  
(Cisco Unified IP Phone 7911G only) Connect a Category 3 or 5 straight-through Ethernet cable from another network device, such as a desktop computer, to the 10/100 PC port.  
(Optional) You can connect another network device later if you do not connect one now.

**Related Topics**

- Before You Begin, on page 39  
- Mount Phone on Wall, on page 49  
- Network Settings, on page 50  
- Network and Access Ports, on page 41  
- Cisco Unified IP Phone Power, on page 29  
- Cisco Unified IP Phone 7906G Installation, on page 47  
- Cisco Unified IP Phone 7911G Installation, on page 48
Footstand Installation

The following figures show how to install the footstand on the Cisco Unified IP Phone 7906 and 7911, respectively.

*Figure 1: Connecting the Footstand (Cisco Unified IP Phone 7906G Shown)*

*Figure 2: Connecting the Footstand (Cisco Unified IP Phone 7911G Shown)*
Cisco Unified IP Phone 7906G Installation

The following graphic and table show how to connect the Cisco Unified IP Phone 7906G.
The following graphic and table show how to connect the Cisco Unified IP Phone 7911G:  

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Network port (10/100 SW)</td>
<td></td>
<td>AC power cord</td>
</tr>
<tr>
<td>2</td>
<td>Handset port</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>DC adapter port (DC48V)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Cisco Unified IP Phone 7911G Installation**

The following graphic and table show how to connect the Cisco Unified IP Phone 7911G:
Mount Phone on Wall

You can mount the Cisco Unified IP Phones on a wall by using the back of the phone as a mounting bracket or you can use special brackets available in a Cisco Unified IP Phones wall mount kit. Wall mount kits must be ordered separately from the phones. If you attach the phone to a wall by using the back of the phone 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

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, refer to the Installing the Universal Wall Mount Kit for the Cisco Unified IP Phone document at: http://www.cisco.com/en/US/products/hw/phones/ps379/prod_installation_guides_list.html

Caution

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Remove the footstand if it is attached to the phone.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Insert two screws into a wall stud, matching them to the two screw holes on the back of the phone.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Hang the phone on the wall.</td>
</tr>
</tbody>
</table>

Phone Startup Verification

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 blink or flash on and off:
   - Handset light strip
   - Hold button
   - Applications Menu button

2. The screen displays the Cisco Systems, Inc., logo screen.

3. These messages display as the phone starts:
   - Configuring IP
   - Updating Trust List
   - Verifying Load
   - Configuring CM List
   - Registering

4. The main screen displays:
   - Current date and time
   - Directory number
   - Softkeys

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 179.

Network Settings

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

- IP address
• IP subnet information
• Default gateway IP address
• Domain name
• DNS server IP address
• TFTP server IP address

Related Topics
Cisco Unified IP Phone Settings, on page 53

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 IP Phone Security Features, on page 10. Also, see the Cisco Unified Communications Manager Security Guide.

Install Locally Significant Certificate

You can install an 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.

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 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.
• The phone should have the correct load file. To verify the image, press the Applications Menu button and choose Settings > Model Information.

For more information, see the 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 Applications Menu and choose Settings > Security Configuration.

Note You can control access to the Settings Menu 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 55 for information 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 that 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. You can stop the process at any time by pressing Stop 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 upgrading. Refer to error messages generated on the CAPF server and take appropriate actions.

You can verify that an LSC is installed on the phone by pressing Applications Menu, then choosing Settings > Model Information, and ensuring that the LSC setting shows Installed.

Related Topics

Cisco Unified IP Phone Security Features, on page 10
CiscoUnifiedIPPhoneSettings

- Phone Settings Overview, page 53
- Cisco Unified IP Phones 7906G and 7911G Menus, page 53
- Phone Setup Options, page 56
- Network Configuration Menu, page 57
- Device Configuration Menu, page 69
- Security Configuration Menu, page 89

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 Phones 7906G and 7911G Menus

The Cisco Unified IP Phone includes the following configuration menus:

- Network Configuration: Provides options for viewing and making a variety of network settings.
- Device Configuration: Provides access to sub-menus from which you can view a variety of non-network-related settings.
- Security Configuration: Provides options for displaying and modifying security settings.

Before you can change option settings on the Network Configuration menu, you must unlock options for editing.

You can control whether a phone user has access to phone settings by using the Settings Access field in the Cisco Unified Communications Manager Administration Phone Configuration Settings window. See Cisco Unified Communications Manager Administration Guide for more information.
Display Settings Menu

To display a configuration menu, perform the following steps.

**Note**

You can control whether a phone has access to the Settings menu or to options on this menu by using 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 *Applications Menu*.

**Step 2**  Choose *Settings*.

**Step 3**  Perform one of these actions to display the desired menu:

- Use *Navigation* to select the desired menu and then press *Select*.
- Use the keypad on the phone to enter the number that corresponds to the menu.

**Step 4**  To display a submenu, repeat Step 3.

**Step 5**  To exit a menu, press *Exit*.

**Related Topics**

- Unlock and Lock Options, on page 55
- Value Input Guidelines, on page 55
- Phone Setup Options, on page 56
- Network Configuration Menu, on page 57
- Device Configuration Menu, on page 69
- Security Configuration Menu, on page 89
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, as shown next.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>⚒️</td>
<td>Option is locked</td>
</tr>
<tr>
<td>🕳️</td>
<td>Option is unlocked</td>
</tr>
</tbody>
</table>

Procedure

**Step 1**
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 **#**.

**Step 2**
After you have made your changes, lock the options by pressing **#**.

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

Related Topics

- Display Settings Menu, on page 54
- Value Input Guidelines, on page 55
- Phone Setup Options, on page 56
- Network Configuration Menu, on page 57
- Device Configuration Menu, on page 69

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 "e." 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 pressing the Save softkey to discard any changes that you have made.

Note

The Cisco Unified IP Phone provides several methods that you can use to reset or restore option settings, if necessary. For more information, see Cisco Unified IP Phone Reset or Restore, on page 197.

Related Topics

Display Settings Menu, on page 54
Unlock and Lock Options, on page 55
Phone Setup Options, on page 56
Network Configuration Menu, on page 57
Device Configuration Menu, on page 69

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 57.

Note

There are several options on the Network Configuration menu and on the Device Configuration Menu that are for display only or that you can configure from Cisco Unified Communications Manager. These options are also described in the Network Configuration Menu, on page 57 and the or the Device Configuration Menu, on page 69.

Table 10: Configurable Settings

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Network Configuration menu option</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Network 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 (applies to 7911G only)</td>
</tr>
</tbody>
</table>
## Network Configuration Menu

The Network Configuration menu provides options for viewing and making a variety of network settings. The following tables describe these options and, where applicable, explain how to change them.

For information about how to access the Network Configuration menu, see Display Settings Menu, on page 54.

### Category | Description | Network Configuration menu option
--- | --- | ---
Port settings | Allows you to set the speed and duplex of the network and access ports. | SW Port Configuration
 |  | PC Port Configuration (applies to 7911G only)

### IPv4 Network Settings

| DHCP settings | 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. | DHCP
 |  | DHCP Address Released

IP settings | If you do not use DHCP in your network, you can make IP settings manually. | Domain Name
 |  | IP Address
 |  | Subnet Mask
 |  | Default Router 1-5
 |  | DNS Server 1-5

TFTP settings for TFTP IPv4 servers | 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. | Alternate TFTP
 |  | TFTP Server 1
 |  | TFTP Server 2

### Related Topics
- Display Settings Menu, on page 54
- Unlock and Lock Options, on page 55
- Value Input Guidelines, on page 55
- Network Configuration Menu, on page 57
- Device Configuration Menu, on page 69
Before you can change an option on this menu, you must unlock options as described in the Unlock and Lock Options, on page 55. The Edit, Yes, or No softkeys for changing 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 55.

**Table 11: Network Configuration menu options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 Configuration</td>
<td>Internet Protocol v4 address menu. In the IPv4 Configuration menu, you can do the following:</td>
<td>Set IPv4 Configuration Fields, on page 63</td>
</tr>
<tr>
<td></td>
<td>• Enable or disable the phone to use the IPv4 address that is assign by the DHCPv4 server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Manually set the IPv4 Address, Subnet Mask, Default Routers, DNSv4 Server, and Alternate TFTP servers for IPv4.</td>
<td></td>
</tr>
<tr>
<td>IPv6 Configuration</td>
<td>Internet Protocol v6 address menu. Enable or disable the phone to use the IPv6 address that is assigned by the DHCPv6 server or to use the IPv6 address that it acquires through Stateless Address Autoconfiguration (SLAAC). For more information on SLAAC, see Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager.</td>
<td></td>
</tr>
<tr>
<td>MAC Address</td>
<td>Unique Media Access Control (MAC) address of the phone.</td>
<td>Display only—Cannot configure.</td>
</tr>
<tr>
<td>Host Name</td>
<td>Unique host name that the DHCP server assigned to the phone.</td>
<td>Display only—Cannot configure.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Name of the Domain Name System (DNS) domain in which the phone resides.</td>
<td>Set Domain Name Field, on page 64</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If the phone receives different domain names from the DHCPv4 and DHCPv6 servers, the domain name from the DHCPv6 takes precedence.</td>
<td></td>
</tr>
</tbody>
</table>
### Operational VLAN ID

**Description**

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.

**To change**

The phone obtains its Operational VLAN ID via 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.

### Admin. VLAN ID

**Description**

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.

**To change**

Set Admin VLAN ID Field, on page 64

### SW Port Configuration

**Description**

Speed and duplex of the network port. Valid values:

- Auto Negotiate
- 10 Half—10-BaseT/half duplex
- 10 Full—10-BaseT/full duplex
- 100 Half—100-BaseT/half duplex
- 100 Full—100-BaseT/full duplex
- 1000 Full—1000-BaseT/full duplex

If the phone is connected to a switch, configure the port on the switch to the same speed/duplex as the phone, or configure both to autonegotiate.

If you change the setting of this option, you must change the PC Port Configuration option to the same setting.

**To change**

Set SW Port Configuration Field, on page 65
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
<tbody>
<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 65</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 autonegotiate. If you change the setting of this option, you must change the SW Port Configuration option to the same setting.</td>
<td></td>
</tr>
<tr>
<td>PC VLAN</td>
<td>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.</td>
<td>Set PC VLAN Field, on page 66</td>
</tr>
</tbody>
</table>

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. When DHCP is enabled, the DHCP server assigns the phone an IPv4 address. When DHCP is disabled, you must manually assign an IPv4 address to the phone.</td>
<td>Set DHCP Field, on page 66</td>
</tr>
<tr>
<td>IP Address</td>
<td>Internet Protocol version 4 (IPv4) address of the phone. If you assign an IPv4 address with this option, you must also assign a subnet mask and default router. See the Subnet Mask and Default Router options in this table.</td>
<td>Set IP Address Field, on page 66</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Subnet mask used by the phone.</td>
<td>Set Subnet Mask Field, on page 67</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>To Change</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</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 67</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>DNS Server 1</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>
<td>Set DNS Server Fields, on page 67</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 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>DHCP Address Released</td>
<td>Releases the IPv4 address assigned by DHCP.</td>
<td>Set DHCP Address Released Field, on page 68</td>
</tr>
<tr>
<td>Alternate TFTP</td>
<td>Indicates whether the phone is using an alternative TFTP server.</td>
<td>Set Alternate TFTP Field, on page 68</td>
</tr>
</tbody>
</table>
To Change

Description

Primary Trivial File Transfer Protocol (TFTP) server used by the phone. If you are not using DHCP in your network and you want to change this server, you must use the TFTP Server 1 option.

If you set the Alternate TFTP option to yes, you must enter a nonzero value for the TFTP Server 1 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 either of the files before you can save changes to the TFTP Server 1 option. In this case, the phone deletes either of the files when you save changes to the TFTP Server 1 option. A new CTL or ITL file is downloaded from the new TFTP Server 1 address.

When the phone looks for its TFTP server, the phone 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

Note: For information about the CTL and ITL files, 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 91.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>TFTP Server 1</td>
<td>Primary Trivial File Transfer Protocol (TFTP) server used by the phone.</td>
<td>Set TFTP Server 1 Field, on page 68</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 TFTP Server 1 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 TFTP Server 1 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 either of the files before you can save changes to the TFTP Server 1 option. In this case, the phone deletes either of the files when you save changes to the TFTP Server 1 option. A new CTL or ITL file is downloaded from the new TFTP Server 1 address.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>When the phone looks for its TFTP server, the phone 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. Manually assigned IPv6 TFTP Servers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. 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 and ITL files, see Unlock CTL and ITL Files, on page 91.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>TFTP Server 2</td>
<td>Optional backup TFTP server that the phone uses if the primary TFTP server is unavailable. 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 either of the files before you can save changes to the TFTP Server 2 option. In this case, the phone deletes either of the files when you save changes to the TFTP Server 2 option. A new CTL or ITL file is downloaded from the new TFTP Server 2 address. When the phone looks for its TFTP server, the phone 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 the CTL and ITL files, see Unlock CTL and ITL Files, on page 91.</td>
<td>Set TFTP Server 2 Field, on page 69</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>

## Set IPv4 Configuration Fields

### Procedure

**Step 1** Unlock network configuration options.

**Step 2** Scroll to IPv4 Configuration and press the Select softkey.
Set Domain Name Field

Procedure

Step 1 Unlock network configuration options.
Step 2 To disable DHCP, perform one of the following actions:
   • If the IP Addressing mode is configured for IPv4 only, set the DHCP option to No.
   • If the IP Addressing mode is configured for IPv6 only, set the DHCPv6 option to No.
   • If the IP Addressing mode is configured for both IPv4 and IPv6, set both DHCP option and DHCPv6 to No.

Step 3 Scroll to the Domain Name option.
Step 4 Press Edit.
Step 5 Enter a new domain name.
Step 6 Press Validate.
Step 7 Press Save.

Set Admin VLAN ID Field

Procedure

Step 1 Unlock network configuration options.
Step 2 Scroll to the Admin. VLAN ID option.
Step 3 Press Edit.
Step 4 Enter a new Admin VLAN setting.
Step 5 Press Validate.
Step 6 Press Save.
Set SW Port Configuration Field

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</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>Action</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**

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

Set DHCP Field

**Procedure**

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

Set IP Address Field

**Procedure**

1. Unlock network configuration options.
2. Set the DHCP option to No.
3. Scroll to the IP Address option, press Edit and enter a new IP Address.
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 No.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Scroll to the Subnet Mask option, press Edit, and then enter a new subnet mask.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Press Validate and then press Save.</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 No.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Scroll to the appropriate Default Router option, press Edit, and then enter a new router IP address.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Press Validate.</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 Save.</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 No.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Scroll to the appropriate DNS Server option, press Edit, and then enter a new DNS server IP address.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Press Validate.</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 Save.</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**.

Device Configuration Menu

The Device Configuration menu provides access to 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.

For instructions about how to access the Device Configuration menu and its sub-menus, see Display Settings Menu, on page 54.

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 Cisco Unified Communications Manager servers that are available for processing calls from the phone, in prioritized order. To change these options, use Cisco Unified Communications Manager Administration.

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 13: 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>State</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------------------------------------------------------------</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 14: 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 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. For more information, see &quot;Survivable Remote Site Telephony Configuration&quot; 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 that it registered with the TFTP server instead.</td>
</tr>
<tr>
<td>🗝️</td>
<td>Indicates that the call is from a trusted device, and that the connection to the Cisco Unified Communications Manager is authenticated. For more information about authentication, see Cisco Unified Communications Manager Security Guide.</td>
</tr>
<tr>
<td>🗝️</td>
<td>Indicates that the call is from a trusted device, and that the connection to the Cisco Unified Communications Manager is authenticated and encrypted. For more information about authentication and encryption, see 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 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.

### SIP General Configuration Menu

The SIP General Configuration menu displays information about the configurable SIP parameters on the phone. The following table describes the options in this menu.
<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.</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) supports out-of-band signaling by using the AVT tone method. Valid values are none, avt, and avt_always.</td>
<td>Display only—cannot configure.</td>
</tr>
<tr>
<td>Register with Proxy</td>
<td>This value is 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 display on the phone. This text is for user display only and has no effect on caller identification or messaging.</td>
<td>Display only—cannot configure.</td>
</tr>
<tr>
<td>Enable VAD</td>
<td>The default value is set to No.</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>
<tr>
<td>End Media Port</td>
<td>Displays the end 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>
<tr>
<td>NAT Enabled</td>
<td>Displays if Network Address Translation (NAT) is enabled.</td>
<td>Display only—cannot configure.</td>
</tr>
<tr>
<td>NAT Address</td>
<td>Displays the WAN IP address of the NAT or firewall server.</td>
<td>Display only—cannot configure.</td>
</tr>
<tr>
<td>Call Statistics</td>
<td>The default value is set to No.</td>
<td>From Cisco Unified Communications Manager Administration, choose Device &gt; Device Settings &gt; SIP Profile.</td>
</tr>
</tbody>
</table>
Related Topics

- Display Settings Menu, on page 54
- Device Configuration Menu, on page 69

Line Settings Menu for SIP Phones

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

**Table 16: Line Settings Menu Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</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>Short Name</td>
<td>Displays the short name configured for the line.</td>
<td>Use Cisco Unified Communications Manager Administration to modify.</td>
</tr>
</tbody>
</table>
| Longer Authentication Name | Displays the name used by the phone for authentication if a registration is challenged by the proxy server during initialization.  
Cisco Unified IP Phone 7900 Series using SIP can have an authentication name up to 128 characters long. The authentication name is used to verify that the phone is allowed to send SIP messages (REGISTER, INVITE, and SUBSCRIBE) to the Cisco Unified Communications Manager. | Use Cisco Unified Communications Manager Administration to modify.                             |
| Authentication Password | Displays the password used by the phone for authentication if a registration is challenged by the proxy server during initialization.                                                                                                                                                                                                 | Use Cisco Unified Communications Manager Administration to modify.                             |
| Display Name         | Displays the identification the phone uses for display for caller identification purposes.                                                                                                                                                                                                                                                  | Use Cisco Unified Communications Manager Administration to modify.                             |
| Proxy Address        | Displays the IP address of the proxy server that will be used by the phone. The value is left blank because it is not applicable to SIP phones that are using Cisco Unified Communications Manager.                                                                                                                          | Display only—cannot configure.                                                                 |

Cisco Unified IP Phone 7906G and 7911G Administration Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)
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 17: 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 Device &gt; Device Settings &gt; SIP Profile.</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 Device &gt; Device Settings &gt; SIP Profile.</td>
</tr>
<tr>
<td>Call Waiting</td>
<td>Indicates whether Call Waiting is enabled (Yes) or disabled (No) for the phone.</td>
<td>From Cisco Unified Communications Manager Administration, choose Call Routing &gt; Directory Number.</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 Device &gt; Device Settings &gt; SIP Profile.</td>
</tr>
<tr>
<td>Shutter Msg Waiting</td>
<td>Indicates whether shutter message waiting is enabled (Yes) or disabled (No) for the phone.</td>
<td>From Cisco Unified Communications Manager Administration, choose Device &gt; Device Settings &gt; SIP Profile.</td>
</tr>
<tr>
<td>Auto Answer Preferences</td>
<td>Indicates whether AutoAnswer is enabled (Yes) or disabled (No) for the phone.</td>
<td>From Cisco Unified Communications Manager Administration, choose Call Routing &gt; Directory Number.</td>
</tr>
</tbody>
</table>
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.

Note

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>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Speed Dials</td>
<td>Indicates whether Speed Dial is enabled (Yes) or disabled (No) for the phone.</td>
<td>From Cisco Unified Communications Manager Administration, choose Device &gt; Phone &gt; Add a New Speed Dial.</td>
</tr>
<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>
</tbody>
</table>
To change Description Option
From Cisco UnifiedCommunicationsManager Administration, choose Device > Phone > PhoneConfiguration.

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.

From Cisco UnifiedCommunicationsManager Administration, choose Device > Phone > PhoneConfiguration.

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 UnifiedCommunicationsManager Administration, choose Device > Phone > PhoneConfiguration.

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 UnifiedCommunicationsManager Administration, choose Device > Phone > PhoneConfiguration.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
<tbody>
<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 UnifiedCommunicationsManager Administration, choose Device &gt; Phone &gt; PhoneConfiguration.</td>
</tr>
<tr>
<td>Idle URL</td>
<td>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.</td>
<td>From Cisco UnifiedCommunicationsManager Administration, choose Device &gt; Phone &gt; PhoneConfiguration.</td>
</tr>
<tr>
<td>Idle URL Time</td>
<td>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.</td>
<td>From Cisco UnifiedCommunicationsManager Administration, choose Device &gt; Phone &gt; PhoneConfiguration.</td>
</tr>
</tbody>
</table>

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 19: 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 installing user locale, see the Cisco Unified Communications Operating System Administration Guide.</td>
<td>From Cisco UnifiedCommunicationsManager Administration, choose Device &gt; Phone &gt; PhoneConfiguration.</td>
</tr>
</tbody>
</table>
The UI Configuration menu displays whether the group listen function is enabled.

**Table 20: UI Configuration Menu Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
<tbody>
<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 Char Set</td>
<td>Character set that the phone uses for the user locale.</td>
<td>Display only—cannot configure.</td>
</tr>
<tr>
<td>Network Locale</td>
<td>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.</td>
<td>From Cisco Unified Communications Manager Administration, choose <strong>Device &gt; Phone &gt; Phone Configuration</strong>.</td>
</tr>
<tr>
<td>Network Locale Version</td>
<td>Version of the network locale loaded on the phone.</td>
<td>Display only—cannot configure.</td>
</tr>
<tr>
<td>NTP Configuration (SIP phones only)</td>
<td>Menu to view information on NTP server and mode configuration. For more information, see NTP Configuration Menu for SIP Phones, on page 79.</td>
<td>From Cisco Unified Communications Manager Administration, choose <strong>System &gt; Phone NTP Reference</strong>.</td>
</tr>
</tbody>
</table>

**UI Configuration Menu**

The UI Configuration menu displays whether the group listen function is enabled.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Listen, Enabled/Disabled</td>
<td>Indicates whether the group listen feature is enabled or disabled.</td>
<td>From Cisco Unified Communications Manager Administration, choose <strong>Device &gt; Phone &gt; Phone Configuration</strong>.</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: <strong>Lower</strong>: Focus priority given to incoming calls. <strong>Higher</strong>: Focus priority given to reverting calls. <strong>Even</strong>: Focus priority given to the first call.</td>
<td>Use Cisco Unified Communications Manager to modify options. See Hold Reversion in Telephony Features Available for Cisco Unified IP Phone, on page 98.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>To change</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</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 are disabled regardless of the settings. Default: Enabled.</td>
<td>From Cisco Unified Communications Manager Administration, choose Device &gt; Phone &gt; Phone Configuration.</td>
</tr>
<tr>
<td>&quot;more&quot; Softkey Timer</td>
<td>Indicates the number of seconds that additional softkeys are displayed 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>Wideband Handset UI Control</td>
<td>Indicates whether the user can configure the Wideband Handset option in the phone user interface. Values:</td>
<td>From Cisco Unified Communications Manager Administration, choose Device &gt; Phone &gt; Phone Configuration.</td>
</tr>
<tr>
<td></td>
<td>• Enabled: The user can configure the Wideband Handset option in the Audio Preferences menu on the phone (choose User Preferences &gt; Audio Preferences &gt; Wideband Handset).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Disabled: The value of the Wideband Handset option in Cisco Unified Communications Manager Administration gets used (see Media Configuration Menu, on page 78).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Default: Enabled</td>
<td></td>
</tr>
<tr>
<td>Personalization</td>
<td>Indicates whether the user can configure custom ring tones and wallpaper images.</td>
<td>From Cisco Unified Communications Manager Administration, choose Device &gt; Phone &gt; Phone Configuration.</td>
</tr>
<tr>
<td>Enbloc Dialing (SCCP only)</td>
<td>Indicates whether the phone will use Enbloc Dialing. If Enabled, the phone will use Enbloc Dialing when possible. If Disabled, the phone will not use Enbloc dialing. You should disable Enbloc Dialing if either Forced Authorization Codes (FAC) or Client Matter Codes (CMC) dialing is being used. Default: Enabled</td>
<td>From Cisco Unified Communications Manager Administration, choose Device &gt; Phone &gt; Phone Configuration.</td>
</tr>
</tbody>
</table>
Media Configuration Menu

The Media Configuration menu displays whether the speaker capability is enabled. The following table describes the options on this menu.

Table 21: Media Configuration Menu Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Speaker Enabled</td>
<td>Indicates whether the speaker is enabled for monitoring calls on the phone.</td>
<td>From Cisco Unified Communications Manager Administration, choose <strong>Device &gt; Phone &gt; Phone Configuration</strong>.</td>
</tr>
<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 <strong>User Preferences &gt; Audio Preferences &gt; Wideband Handset</strong>.</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>• If Wideband Handset UI Control is disabled, from Cisco Unified Communications Manager Administration, choose <strong>Device &gt; Phone &gt; Phone Configuration</strong> to set this value.</td>
</tr>
<tr>
<td>Enterprise Advertise</td>
<td>Enables/disables Cisco Unified IP Phones to advertise the G.722 codec to Cisco Unified Communications Manager. For more information, see Cisco Unified Communications Manager System Guide, “Cisco Unified IP Phones” chapter.</td>
<td>From Cisco Unified Communications Manager Administration, choose <strong>System &gt; Enterprise Parameters</strong>.</td>
</tr>
<tr>
<td>G.722 Codec</td>
<td></td>
<td>Note: If you allow the user to change the Wideband Handset UI Control option, the user-configured value takes precedence.</td>
</tr>
<tr>
<td></td>
<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>
</tr>
</tbody>
</table>

Note: If Wideband Handset UI Control is enabled, you or the user can choose **User Preferences > Audio Preferences > Wideband Handset**.
NTP Configuration Menu for SIP Phones

The NTP Configuration menu, which opens when you select NTP Configuration on the Locale Configuration menu, displays information about the NTP server and mode configuration used by the phone. The following table describes the options on this menu. For more information, see Locale Configuration Menu, on page 75.

Table 22: NTP Configuration Menu Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Advertise G.722 Codec</td>
<td>Allows you to override the Enterprise Advertise G.722 Codec on a per-phone basis. Default: 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>

Ethernet Configuration Menu

The Ethernet Configuration menu includes the options that are described in the following table.
Table 23: Ethernet Configuration menu option

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Span to PC Port (applies to 7911G only)</td>
<td>Indicates whether the phone forwards packets transmitted and received on the network port to the access port. Enable this option if an application that requires monitoring of the phone traffic is being run 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. When Span to PC Port is enabled, the PC attached to the Cisco Unified IP Phone 7911 cannot authenticate using 802.1x.</td>
<td>From Cisco Unified Communications Manager Administration, choose Device &gt; Phone &gt; Phone Configuration.</td>
</tr>
</tbody>
</table>
| Forwarding Delay (applies to 7911G only) | Indicates whether the internal switch begins forwarding packets between the PC port and switched port on the phone when the phone becomes active.  
  • When forwarding delay is set to disabled, the internal switch begins forwarding packets immediately.  
  • When forwarding delay is set to enabled, the internal switch waits 8 seconds before forwarding packets between the PC port and the switch port.  
  Default is disabled.                                                                                                                                                                                                                                                                                                                                     | From Cisco Unified Communications Manager Administration, choose Device > Phone > Phone Configuration.                                                                                                                                                                                                                                                                                                                                                      |

**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 89.

The following table describes the Security Configuration menu options.
### Table 24: 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 (applies to 7911G only)</td>
<td>Indicates whether the access port on the phone is enabled (No) or disabled (Yes).</td>
<td>From Cisco Unified Communications Manager Administration, choose <strong>Device &gt; Phone &gt; Phone Configuration</strong>.</td>
</tr>
<tr>
<td>GARP Enabled</td>
<td>Indicates whether the phone learns MAC addresses from GARP responses. Disabling the phone’s ability to accept GARP will prevent applications that use this mechanism to monitor and record voice streams from working. If voice monitoring is not desired, set this option to No (disabled).</td>
<td>From Cisco Unified Communications Manager Administration, choose <strong>Device &gt; Phone &gt; Phone Configuration</strong>.</td>
</tr>
<tr>
<td>Voice VLAN Enabled (applies to 7911G only)</td>
<td>Indicates whether the phone allows a device attached to the access port to access the Voice VLAN. 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 sent and received by the phone. Setting this option to Yes (enabled) if an application that requires monitoring of the phone’s traffic is running on the PC. These applications include monitoring and recording applications and network monitoring software.</td>
<td>From Cisco Unified Communications Manager Administration, choose <strong>Device &gt; Phone &gt; Phone Configuration</strong>.</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 <strong>Control Web Page Access</strong>, on page 165.</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>Used by Cisco Technical Assistance Center (TAC) for troubleshooting. The Cisco Unified IP Phone 7911G can be configured for Enabled, Disabled, or PC Controlled. The Cisco Unified IP Phone 7906G supports only Enabled or Disabled (no PC Controlled).</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 QoS Configuration menu options.

Table 25: 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>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 54
Network Configuration Menu, on page 57

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 from the main menu. For information about the options on that menu, see Network Configuration Menu, on page 57.
Table 26: 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, negating the need to traverse the WAN link for the upgrade of each phone. 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. <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>From Cisco Unified Communications Manager Administration, choose <strong>Device &gt; Phone &gt; Phone Configuration.</strong></td>
</tr>
<tr>
<td>IPv6 Load Server</td>
<td>This feature is disabled in this release.</td>
<td></td>
</tr>
<tr>
<td>RTP Control Protocol</td>
<td>Indicates whether the phone supports the Real Time Control Protocol. Settings include: • Enabled • Disabled (default) If this feature is disabled, several call statistic values display as 0. For additional information, see the following sections: • <a href="#">Call Statistics Screen, on page 157</a> • <a href="#">Streaming Statistics, on page 175</a></td>
<td>From Cisco Unified Communications Manager Administration, choose <strong>Device &gt; Phone &gt; Phone Configuration.</strong></td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>To change</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CDP: SW Port</td>
<td>Indicates whether CDP is enabled on the switch port (default is enabled).</td>
<td>Use Cisco Unified Communications Manager Administration, and choose Device &gt; Phone &gt; Phone Configuration.</td>
</tr>
<tr>
<td></td>
<td>• Enable CDP on the switch port for VLAN assignment for the phone, power negotiation, QoS management, and 802.1x security.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enable CDP on the switch port when the phone is connected to a Cisco switch.</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>When CDP is disabled in Cisco Unified Communications Manager, a warning is presented, indicating that CDP should be disabled on the switch port only if the phone is connected to a non-Cisco switch.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The current PC and switch port CDP values are shown on the Settings menu.</td>
<td></td>
</tr>
</tbody>
</table>
To change Description Option
Use Cisco Unified Communications Manager Administration, and choose
Device &gt; Phone &gt; Phone Configuration.

<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>Use Cisco Unified Communications Manager Administration, and choose Device &gt; Phone &gt; Phone Configuration.</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 simultaneously</td>
<td></td>
</tr>
</tbody>
</table>
|                     | Peer Firmware Sharing may also aid in firmware upgrades in branch or remote office deployment scenarios over bandwidth-limited WAN links. When enabled, it 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. The individual files making up the firmware image are retrieved from the TFTP server by only the root phone in the hierarchy, and are then rapidly transferred down the transfer hierarchy to the other phones on the subnet using TCP connections. This menu option indicates whether the phone supports peer firmware sharing. Settings include:
<p>|                     | • Enabled (default)                                                        |                                                                           |
|                     | • Disabled                                                                 |                                                                           |
| Log Server          | Indicates the IP address and port of the remote logging machine to which the phone sends log messages. These log messages help in debugging the peer to peer image distribution feature. <strong>Note</strong>: The remote logging setting does not affect the sharing log messages sent to the phone log. | Use Cisco Unified Communications Manager Administration, and choose Device &gt; Phone &gt; Phone Configuration. |
| IPv6 Log Server      | This feature is disabled in this release.                                 |                                                                           |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDP: PC Port (applies to 7911G only)</td>
<td>Indicates whether CDP is enabled on the PC port (default is enabled).</td>
<td>Use Cisco Unified Communications Manager Administration, and choose Device &gt; Phone.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> When CDP is disabled in Cisco Unified Communications Manager, a warning is displayed, indicating that disabling CDP on the PC port prevents CVTA from working.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The current PC and switch port CDP values are shown on the Settings menu.</td>
<td></td>
</tr>
<tr>
<td>LLDP: PC Port</td>
<td>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, which should match the protocol supported by the switch. Settings include:</td>
<td>Use Cisco Unified Communications Manager Administration, and choose Device &gt; Phone &gt; Phone Configuration</td>
</tr>
<tr>
<td></td>
<td>• Enabled (default)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Disabled</td>
<td></td>
</tr>
<tr>
<td>LLDP-MED: SW Port</td>
<td>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:</td>
<td>Use Cisco Unified Communications Manager Administration, and choose Device &gt; Phone &gt; Phone Configuration</td>
</tr>
<tr>
<td></td>
<td>• Enabled (default)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Disabled</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>LLDP Power Priority</td>
<td>Advertises the phone power priority to the switch, enabling the switch to</td>
<td>Use Cisco Unified Communications Manager Administration, and choose Device &gt; Phone &gt; Phone Configuration</td>
</tr>
<tr>
<td></td>
<td>appropriately provide power to the phones. Settings include:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Unknown (default)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Low</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• High</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Critical</td>
<td></td>
</tr>
<tr>
<td>LLDP Asset ID</td>
<td>Identifies the asset ID assigned to the phone for inventory management.</td>
<td>Use Cisco Unified Communications Manager Administration, and choose Device &gt; Phone &gt; Phone Configuration</td>
</tr>
<tr>
<td>IP Addressing Mode</td>
<td>Displays the IP addressing mode that is available on the phone—IPv4 only,</td>
<td>From Cisco Unified Communications Manager Administration, choose Device &gt; Device Settings &gt; Common Device Configuration.</td>
</tr>
<tr>
<td></td>
<td>IPv6 only, or IPv4 and IPv6.</td>
<td></td>
</tr>
<tr>
<td>IP Addressing Mode Preference for Signaling</td>
<td>Indicates the IP address version that the phone uses during signaling with Cisco Unified Communications Manager when IPv4 and IPv6 are both available on the phone.</td>
<td>From Cisco Unified Communications Manager Administration, choose Device &gt; Device Settings &gt; Common Device Configuration.</td>
</tr>
</tbody>
</table>
### Auto IP Configuration
Displays whether autoconfigurations is enabled or disabled on the phone.

The Auto IP Configuration setting along with the DHCPv6 setting determine how the IP Phone obtains its IPv6 address and other network settings. For more information on how these two settings affect the network settings on the phone, see Unified CM Configuration Menu, on page 69.

**Note** Use the Allow Auto-Configuration for Phones setting in Cisco Unified Communications Manager Administration.

### IPv6 Load Server
Used to optimize installation time for phone firmware upgrades and off-load the WAN by storing images locally, negating the need to traverse the WAN link for the upgrade of each phone.

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.

**Note** When you configure both an IPv6 Load Server and a Load Server (for IPv4), the IPv6 Load server takes precedence.

From Cisco Unified Communications Manager Administration, choose **Device > Device Settings > Common Device 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 in debugging the peer to peer image distribution feature. 

**Note**

The remote logging setting does not affect the sharing log messages sent to the phone log.

**Use Cisco Unified Communications Manager Administration to modify.**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 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 in debugging the peer to peer image distribution feature.</td>
<td>Use Cisco Unified Communications Manager Administration to modify.</td>
</tr>
</tbody>
</table>

**Related Topics**

- Display Settings Menu, on page 54
- Network Configuration Menu, on page 57

**Security Configuration Menu**

The Security Configuration menu 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 instructions about how to access the Device Configuration menu and its sub-menus, see Display Settings Menu, on page 54.

**Note**

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 80.

The following table describes the options in this 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>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 165.</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 &quot;Using the Certificate Authority Proxy Function&quot; chapter in Cisco Unified Communications Manager Security Guide.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>To change</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</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 MIC for your phone, see the &quot;Using the Certificate Authority Proxy Function&quot; chapter in <em>Cisco Unified Communications Manager Security Guide</em>.</td>
</tr>
<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.</td>
<td>For more information, see Trust List Menu, on page 93.</td>
</tr>
<tr>
<td>IPv6 CAPF Server</td>
<td>Displays the IP address and the port of the IPv6 CAPF server that the phone uses.</td>
<td>For more information about this server, see the &quot;Using the Certificate Authority Proxy Function&quot; chapter in <em>Cisco Unified Communications Manager Security Guide</em>.</td>
</tr>
<tr>
<td>802.1X Authentication</td>
<td>Allows you to enable 802.1X authentication for this phone.</td>
<td>See 802.1X Authentication and Status, on page 94.</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>
</tbody>
</table>

**CTL File Submenu**

The CTL File submenu 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 submenu by pressing **Applications Menu** and choosing **Security Configuration > Trust List**.
### Unlock CTL and ITL Files

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

**Procedure**

**Step 1** Press **##** to unlock options on the overall setting menu of the Cisco Unified IP Phone.

**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 (TVS) does not generate the ITL file, as done in previous releases.

Table 29: ITL File Settings

<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 ITL file that is installed in the phone.</td>
<td>For more information about the CTL file, see the Configuring the &quot;Cisco ITL Client&quot; section in Cisco Unified Communications Manager Security Guide.</td>
</tr>
<tr>
<td></td>
<td>If security is configured for the phone, the ITL file installs automatically when the phone reboots or resets.</td>
<td></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; in Cisco Unified Communications Manager Security Guide.</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.</td>
<td>For information about changing these options, see Network Configuration Menu, on page 57.</td>
</tr>
<tr>
<td></td>
<td>If neither the certificate of TFTP (TFTP Server 1) nor the certificate of backup TFTP (TFTP Server 2) is not in the CTL or ITL file, you must unlock the CTL file.</td>
<td></td>
</tr>
</tbody>
</table>
Trust List Menu

The Trust List menu provides a top-level menu containing 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. The following table describes the options in this menu.

Table 30: Trust List Information

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Server</td>
<td>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.</td>
<td>For more information about phone-trust certificates, see the following manuals:</td>
</tr>
<tr>
<td>Trust Verification Service (TVS) Server</td>
<td>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.</td>
<td>For more information, see the Cisco Unified Communications Manager System Administrator Guide.</td>
</tr>
<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 CTL Client&quot; in Cisco Unified Communications Manager Security Guide.</td>
</tr>
</tbody>
</table>
### 802.1X Authentication and Status

Use the options that are described in the following tables to enable 802.1X authentication and monitor its progress:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
<tbody>
<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 CTL Client&quot; in Cisco Unified Communications Manager Security Guide.</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 CTL Client&quot; in Cisco Unified Communications Manager Security Guide.</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 Cisco Unified IP Phone CTL file. | For more information about phone-trust certificates, see the following manuals:  

### Option | Description | To change
--- | --- | ---
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. | **Set Device Authentication Field**, on page 96 |
### EAP-MD5

Specifies a password for use with 802.1X Authentication using the following menu options (described in the following rows):

- Device ID
- Shared Secret
- Realm

**Device ID:** A derivative of the phone's model number and unique MAC Address displayed in this format: CP-<model>-SEP-<MAC Address>

**Shared Secret:** Choose a password to use on the phone and on the authentication server. The password must be between 6 and 32 characters, consisting of any combination of numbers or letters.

**Note:** If you disable 802.1X authentication or perform a factory reset of the phone, the shared secret is deleted.

**Realm:** Indicates the user network domain, always set as Network.

**To change:**

Choose Settings > Security Configuration > 802.1X Authentication > EAP-MD5.

Display only—Cannot configure.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
<tbody>
<tr>
<td>EAP-MD5</td>
<td>Specifies a password for use with 802.1X Authentication using the following menu options (described in the following rows):</td>
<td>Choose Settings &gt; Security Configuration &gt; 802.1X Authentication &gt; EAP-MD5.</td>
</tr>
<tr>
<td></td>
<td>- Device ID</td>
<td>Display only—Cannot configure.</td>
</tr>
<tr>
<td></td>
<td>- Shared Secret</td>
<td>Set EAP-MD5 Shared Secret Field, on page 96</td>
</tr>
<tr>
<td></td>
<td>- Realm</td>
<td>Display only—Cannot configure.</td>
</tr>
</tbody>
</table>

### Table 31: 802.1X Authentication Status

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

**Table 31: 802.1X Authentication Status**

Display only—Cannot configure.
Set Device Authentication Field

Procedure

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

Set EAP-MD5 Shared Secret Field

See Cisco Unified IP Phone Security Problems, on page 186 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.
CHAPTER 5

Features, Templates, Services, and Users

• Features, Templates, Services, and Users Overview, page 97
• Telephony Features Available for Cisco Unified IP Phone, page 98
• Product-Specific Parameters, page 118
• Corporate and Personal Directory Setup, page 119
• Phone Button Templates, page 120
• Softkey Templates, page 123
• Enable Device Invoked Recording, page 123
• Services Setup, page 124
• Cisco Unified Communications Manager User Addition, page 124
• User Options Web Pages Management, page 125
• EnergyWise Setup on Cisco Unified IP Phone, page 127
• UCR 2008 Setup, page 130

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 communications 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 203

For information about setting up phones in non-English environments, see International User Support, on page 217.
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 contains configuration procedures and related information.

For more information about using most of these features on the phone, see the Cisco Unified IP Phone 7906G and 7911G User Guide for Cisco Unified Communications Manager (SCCP and SIP).

Note
Cisco Unified Communications Manager Administration also provides service parameters that you can use to configure various telephony functions. For more information on accessing and configuring service parameters, see the Cisco Unified Communications Manager Administration Guide. For more information on the functions of a service, click on the name of the parameter or the question mark help button in the Service Parameter Configuration window.

Table 32: Telephony Features for the Cisco Unified IP Phone

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Configuration reference</th>
</tr>
</thead>
</table>
| Abbreviated Dialing| A user can configure up to 99 speed-dial entries. Speed-dial entries that are not assigned to the speed-dial buttons on the phone are used for abbreviated dialing. When a user starts dialing digits, the **AbbrDial** softkey appears, and the user can access any speed-dial entry by entering the appropriate index. **Note** You can use Abbreviated Dialing while on-hook or off-hook. | 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 |
<p>| Add Select to Join | Creates a conference by joining together existing calls that are on a single phone line. | For more information, see the Cisco Unified IP Phone 7906G and 7911G User Guide for Cisco Unified Communications Manager. |</p>
<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. | 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  
To enable Agent Greeting in the Cisco Unified CM Administration application, choose Device > Phone, locate IP Phone that you want to configure. Scroll to the Device Information Layout pane and set Built-in Bridge to On or Default.  
If Built-in Bridge is set to Default, in the Cisco Unified CM Administration application, choose System > Service Parameter and select the appropriate Server and Service. Scroll to the Clusterwide Parameters (Device > Phone) pane and set Built-in Bridge Enable to On. |
| Any Call Pickup     | Allows users to pick up a redirected call via the 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 *Cisco Unified Communications Manager Features and Services Guide*, "Call Pickup" chapter.                                                                                                  |
| Audible Message Waiting Indicator | A stutter tone from the handset, headset, or speakerphone indicates that a user has one or more new voice messages on a line.  
**Note**  
The stutter tone is line-specific. You hear it only when using the line with the waiting messages. | For more information, see :  
• *Cisco Unified Communications Manager Administration Guide*, "Message Waiting Configuration" chapter  
• *Cisco Unified Communications Manager System Guide*, "Voice Mail Connectivity to Cisco Unified Communications Manager" chapter |
<p>| AutoAnswer          | Causes the speakerphone to go off hook automatically when an incoming call is received. The user can monitor the call using the speaker but must pick up the handset to speak to the caller. | For more information, see the <em>Cisco Unified Communications Manager Administration Guide</em>, &quot;Configuring Directory Numbers&quot; chapter.                                                                                      |
| AutoDial            | 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. | No configuration required.                                                                                                                  |</p>
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Configuration reference</th>
</tr>
</thead>
</table>
| Automatic Port Synchronization  | When the Cisco Unified CM 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, Cisco recommends 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 CM, if the phone is powered by PoE.  
**Note** Cisco Unified IP Phone 7906G does not support Automatic Port Synchronization. | To configure the parameter in the Cisco Unified CM 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 an in-progress call on a shared line. 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 <em>Cisco Unified Communications Manager Features and Services Guide</em>, “External Call Transfer Restrictions” chapter. |</p>
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Configuration reference</th>
</tr>
</thead>
</table>
| 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 will alert later participants in the call 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.                                                                                                                                  |
| Call Display Restrictions | Determines the information that displays for calling or connected lines, depending on the parties who are involved in the call.                                                                                                                                                                                                                                                                                  | For more information, see:  
  - *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Configuration" chapter  
  - *Cisco Unified Communications Manager System Guide*, "Understanding Route Plans" chapter  
  - *Cisco Unified Communications Manager Features and Services Guide*, "Call Display Restrictions" chapter.                                                                                                                                                                                  |
| Call Forward     | 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.                                                                                                                                                                                                                          | For more information, see:  
  - *Cisco Unified Communications Manager Administration Guide*, "Directory Number Configuration" chapter  
<p>| Call Forward All Loop Breakout | Detects and prevents Call Forward All loops. When a loop is detected, the Call Forward All configuration is ignored and the call rings through.                                                                                                                                                                                                                                           | For more information, see the <em>Cisco Unified Communications Manager System Guide</em>, &quot;Cisco Unified IP Phones&quot; chapter.                                                                                                                                  |</p>
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Configuration reference</th>
</tr>
</thead>
<tbody>
<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 forward 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>, “Cisco Unified IP Phones” chapter.</td>
</tr>
<tr>
<td>Call Forward 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>, “Understanding Directory Numbers” chapter.</td>
</tr>
<tr>
<td>Call Park</td>
<td>Places the call on hold so that anyone connected to the Cisco Unified Communications Manager system can retrieve the call.</td>
<td>For more information, see:</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If you are using the Park softkey, avoid configuring the Directed Call Park feature. This prevents users from confusing the two Call Park features.</td>
<td>• <em>Cisco Unified Communications Manager System Guide</em>, “Cisco Unified IP Phones” chapter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <em>Cisco Unified Communications Manager Features and Services Guide</em>, “Call Park and Directed Call Park” chapter.</td>
</tr>
<tr>
<td>Call Pickup</td>
<td>Allows users to redirect a call that is ringing on another phone within their pickup group to their phone.</td>
<td>For more information, see the <em>Cisco Unified Communications Manager Features and Services Guide</em>, “Call Pickup Configuration” chapter.</td>
</tr>
<tr>
<td>Call Recording</td>
<td>Enables recording of an active call. The user might hear a recording audible alert tone during a call when it is being recorded.</td>
<td>For more information, see the <em>Cisco Unified Communications Manager Features and Services Guide</em>, “Monitoring and Recording” chapter.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><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></td>
</tr>
<tr>
<td>Call Waiting</td>
<td>Receives a second incoming call on the same line without disconnecting the first call.</td>
<td>For more information, see the <em>Cisco Unified Communications System Guide</em>, “Understanding Directory Numbers” 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>Caller ID</td>
<td>Displays the telephone number and name of the caller.</td>
<td>For more information, see:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cisco Unified Communications Manager Administration Guide, “Directory Number Configuration” chapter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cisco Unified Communications Manager System Guide, “Understanding Route Plans” chapter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cisco Unified Communications Manager Administration Guide, “Directory Number Configuration” chapter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cisco Unified Communications Manager Features and Services Guide, “Call Display Restrictions” chapter</td>
</tr>
<tr>
<td>Caller ID Blocking</td>
<td>Blocks a user's phone number or email address.</td>
<td>For more information, see:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cisco Unified Communications Manager System Guide, “Understanding Route Plans” chapter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cisco Unified Communications Manager Administration Guide, “Directory Number Configuration” chapter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cisco Unified Communications Manager Administration Guide, “SIP Profile Configuration” chapter</td>
</tr>
<tr>
<td>Calling Party</td>
<td>Globalizes or localizes the incoming calling party number so that the</td>
<td>For more information, see the Cisco Unified Communications Features and Services Guide, “Calling Party Normalization” chapter.</td>
</tr>
<tr>
<td>Normalization</td>
<td>appropriate calling number presentation displays on the phone. Supports</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the international escape character plus (+).</td>
<td></td>
</tr>
<tr>
<td>Cisco Call Back</td>
<td>Allows a user to receive call back notification on a Cisco Unified IP Phone</td>
<td>For more information, see:</td>
</tr>
<tr>
<td></td>
<td>when a called party becomes available.</td>
<td>• Cisco Unified Communications Manager System Guide, “Cisco Unified IP Phone Configuration” chapter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cisco Unified Communications Manager Features and Services Guide, “Cisco Call Back” chapter</td>
</tr>
<tr>
<td>Cisco Extension</td>
<td>Enables users to sign into their directory number from any Cisco</td>
<td>For more information, see the Cisco Unified Communications Manager Features and Services Guide, “Cisco Extension Mobility” chapter.</td>
</tr>
<tr>
<td>Mobility</td>
<td>Unified IP 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>Cisco Extension Mobility Change PIN</td>
<td>Enables a user to change the PIN from a Cisco Unified IP Phone. The PIN can be changed by: • Using the Change Credentials service of a Cisco Unified IP Phone • Using the Change PIN softkey on the Extension Mobility logout screen</td>
<td>For more information, see the <em>Cisco Unified Communications Manager Features and Services Guide</em>, “Cisco Extension Mobility” chapter.</td>
</tr>
<tr>
<td>Cisco Extension Mobility Cross Cluster</td>
<td>Enables a user configured in one cluster to log into a Cisco Unified IP Phone in another cluster. Users from a home cluster log into a Cisco Unified IP Phone at a visiting cluster. <strong>Note</strong> Even though the Intercom feature works with Cisco Extension Mobility (EM), it cannot be used with Extension Mobility Cross Cluster (EMCC) because the feature must be enabled with a real phone device. The Intercom feature cannot be enabled with EM profiles.</td>
<td>For more information, see the <em>Cisco Unified Communications Manager Features and Services Guide</em>, “Cisco Extension Mobility Cross Cluster” chapter.</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. <strong>Note</strong> If you are using this feature, you must disable Enbloc dialing. See the “Enbloc Dialing” row in this table for details.</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>Conference</td>
<td>• Allows a user to talk simultaneously with multiple parties by calling each participant individually. Conference features include Conference, Join, cBarge, and Meet Me. • Allows a non-initiator 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.</td>
<td>For more information, see the <em>Cisco Unified Communications Manager System Guide</em>, “Cisco Unified IP Phones” and “Conference Bridges” chapters. The Advance Adhoc Conference service parameter, disabled by default in Cisco Unified Communications Manager Administration, allows you to enable these features. <strong>Note</strong> Be sure to inform your users whether these features are activated.</td>
</tr>
<tr>
<td>Control Default Wallpaper</td>
<td>Administrators can specify the default background image file for the phone in the Cisco Unified Communication Manager 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.</td>
<td>For more information, see the <em>Cisco Unified Communications Manager Features and Services Guide</em>, “Common Phone Profile Configuration” 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>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>
<tr>
<td>Default Audio Path Support</td>
<td>Allows the user to press Answer or a Line button for, and redirect the call to, the last audio path used, by default.</td>
<td>No configuration required.</td>
</tr>
<tr>
<td>Device Invoked Recording</td>
<td>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.</td>
<td>For more information, see <em>Enable Device Invoked Recording</em>, on page 123.</td>
</tr>
<tr>
<td>Directed Call Park</td>
<td>Allows a user to direct an active call to an available directed call park number. After pressing Transfer, the user dials the directed call park number to store the call.</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>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>Direct Transfer</td>
<td>Joins two established calls (calls that are on hold or in connected state) into one call and drops the feature initiator from the call. Does not initiate a consultation call and does not put the active call on hold.</td>
<td>For more information, see the <em>Cisco Unified Communications Manager System Guide</em>, “Cisco Unified IP Phones” chapter.</td>
</tr>
<tr>
<td>Enbloc Dialing (SCCP phones only)</td>
<td>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.</td>
<td>For more information, see <em>Set Up Enbloc Dialing Feature</em>, on page 117</td>
</tr>
<tr>
<td>Distinctive Ring</td>
<td>Users can customize how their phone indicates an incoming call and a new voice mail message.</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. The following DND-related parameters are configurable in Cisco Unified Communications Manager Administration:  
  - Do Not Disturb: This checkbox allows you to enable DND on a per-phone basis. 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, if any, to play 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). | For more information, see the Cisco Unified Communications Manager Features and Services Guide, “Do Not Disturb” chapter. |
| 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.                                                      | For more information, see Phone Power Consumption, on page 21                                               |
| Fast Dial Service            | 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.                                               | For more information, see Phone Button Template for Personal Address Book or Fast Dials, on page 121        |
| Forced Authorization Codes (FAC) (SCCP phones only) | Controls the types of calls that certain users can place.  
  **Note** If you are using this feature, you must disable Enbloc dialing. See Enbloc Dialing in this table for details.                                                                 | For more information, see the Cisco Unified Communications Manager Features and Services Guide, "Client Matter Codes and Forced Authorization Codes" chapter. |
<p>| Group Call Pickup            | Allows a user to answer a call that is ringing on a directory number in another group.                                                                                                                     | For more information, see the Cisco Unified Communications Manager Features and Services Guide, &quot;Call Pickup&quot; chapter. |
| Help System                  | Provides a comprehensive set of topics that appear on the phone screen.                                                                                                                                     | No configuration required.                                                                                     |</p>
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Configuration reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hold/Resume</td>
<td>Allows the user to move a connected call between an active state and a held state.</td>
<td>No configuration required, unless you want to use Music On Hold. See &quot;Music On Hold&quot; in this table for information. See also &quot;Hold Reversion&quot; in this table.</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 as long as the call is 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 about configuring this feature, see the Cisco Unified Communications Manager Features and Services Guide, &quot;Hold Reversion&quot; 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>
</tbody>
</table>
| Hunt Group Display      | 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. | For more information, see:  
  - Cisco Unified Communications Manager Administration Guide, "Hunt Group Configuration" chapter  
  - Cisco Unified Communications Manager System Guide, "Understanding Route Plans" chapter  
  - Cisco Unified Communications Manager Administration Guide, "CTI Route Point Configuration" chapter |
<p>| Immediate Divert        | Allows a user to transfer a ringing, connected, or held call directly to a voicemessaging system. When a call is diverted, the line becomes available to make or receive new calls. | For more information, see the Cisco Unified Communications Manager Features and Services Guide, &quot;Immediate Divert&quot; chapter. |
| Immediate Divert—Enhanced | Allows users to transfer incoming calls directly to their voicemessaging system or to the voice messaging system of the original called party. | For more information, see the Cisco Unified Communications Manager Features and Services Guide, &quot;Immediate Divert&quot; chapter. |</p>
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Configuration reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intelligent Session Control</td>
<td>Reroutes a direct call to user's mobile phone to the enterprise number (desk phone). For an incoming call to remote destination (mobile phone), only remote destination rings; desk phone does not ring. When the call is answered on their mobile phone, the desk phone displays a Remote In Use message. During these calls, users can make use of various features of their 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>Join</td>
<td>Allows users to initiate an ad hoc conference using <strong>Join</strong> softkey. Join does not create a consultation call and does not put the active call on hold. Join can include more than two calls, which results in a call with more than three parties.</td>
<td>For more information, see the <em>Cisco Unified Communications Manager System Guide</em>, “Cisco Unified IP Phones” chapter.</td>
</tr>
<tr>
<td>Log Out of Hunt Groups</td>
<td>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.</td>
<td>For more information, see the <em>Cisco Unified Communications Manager System Guide</em>, “Understanding Route Plans” chapter.</td>
</tr>
</tbody>
</table>
| Malicious Call Identification (MCID) | Allows you to report a call of a malicious nature by requesting that Cisco Unified Communications Manager identify and register the source of an incoming call in the network. | For more information, see:  
  *Cisco Unified Communications Manager System Guide*, “Cisco Unified IP Phones” chapter  
  *Cisco Unified Communications Manager Features and Services Guide*, “Malicious Call Identification” chapter |
| Meet Me Conference            | Enables other callers to join in a conference.                                               | For more information, see:  
  *Cisco Unified Communications Manager Administration Guide*, “Meet-Me Number/Pattern Configuration” chapter  
  *Cisco Unified Communications Manager System Guide*, “Conference Bridges” chapter |
| Message Waiting               | Indicates that one or more voice messages are waiting for a user.                           | For more information, see:  
  *Cisco Unified Communications Manager Administration Guide*, “Message Waiting Configuration” chapter  
  *Cisco Unified Communications Manager System Guide*, “Voice Mail Connectivity to Cisco Unified Communications Manager” chapter |
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Configuration reference</th>
</tr>
</thead>
<tbody>
<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 Cisco Unified Communications Manager Administration Guide, “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 Cisco Unified Communications Manager Features and Services Guide, “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 cellular phone.</td>
<td>For more information, see the Cisco Unified Communications Manager Features and Services Guide, “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 Cisco Unified Communications Manager Features and Services Guide, “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 Cisco Unified Communications Manager Administration Guide, “Cisco Unified IP Phone 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 Cisco Unified Communications Manager Features and Services Guide, “Music On Hold” 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>Mute</td>
<td>Mutes the microphone located in the active handset or headset.</td>
<td>For more information, see the following chapters in <em>Cisco Unified Communications Manager Administration Guide</em>:</td>
</tr>
<tr>
<td></td>
<td>Users can also use the Mute softkey to mute and unmute active calls in off</td>
<td>• &quot;Enterprise Phone Configuration&quot;</td>
</tr>
<tr>
<td></td>
<td>hook, ringing, or connected state.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For the Mute softkey to be displayed in the phone:</td>
<td>• &quot;Common Phone Profile Configuration&quot;</td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified Communications Manager 8.0 and later:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Check the Enable Mute Feature check box in the in one of these windows:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Phone Configuration (Device &gt; Phone)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enterprise Phone Configuration (System &gt; Enterprise Phone Configuration)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Common Phone Profile (Device &gt; Device Settings &gt; Common Phone Profile)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Earlier versions of Cisco Unified Communications Manager:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Check the Enable Mute Feature check box in the Phone Configuration window</td>
<td></td>
</tr>
<tr>
<td></td>
<td>in Cisco Unified Communications Manager Administration.</td>
<td></td>
</tr>
<tr>
<td>On-Hook Call Transfer</td>
<td>Allows a user to press a single Transfer softkey and then go on hook</td>
<td>For more information, see the <em>Cisco Unified Communications Manager System Guide</em>, &quot;Cisco Unified IP Phones” chapter.</td>
</tr>
<tr>
<td></td>
<td>to complete a call transfer.</td>
<td></td>
</tr>
<tr>
<td>On-Hook Predialing</td>
<td>Allows a user to dial a number without going off hook. The user can then</td>
<td>For more information, see the <em>Cisco Unified IP Phone 7906G and 7911G User Guide for Cisco Unified Communications Manager (SCCP and SIP)</em>.</td>
</tr>
<tr>
<td></td>
<td>either pick up the handset or press the Dial softkey.</td>
<td></td>
</tr>
<tr>
<td>Other Group Pickup</td>
<td>Allows a user to answer a call that is ringing on a phone in another 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></td>
<td>that is associated with the user's group.</td>
<td></td>
</tr>
<tr>
<td>Phone Secure Web Access</td>
<td>Cisco Unified IP Phones enable a user to securely access the web with the</td>
<td>For more information, see the <em>Cisco Unified Communications Manager Security Guide</em>, “Phone Security Overview” chapter.</td>
</tr>
<tr>
<td></td>
<td>use of a phone trust store called &quot;phone-trust.&quot;</td>
<td></td>
</tr>
<tr>
<td>Plus Dialing</td>
<td>Allows the user to dial E.164 numbers prefixed with a plus (+) sign.</td>
<td>No configuration required.</td>
</tr>
<tr>
<td></td>
<td>To dial the + sign, the user needs to press and hold the star (*) key for</td>
<td></td>
</tr>
<tr>
<td></td>
<td>at least 1 second. This applies to dialing the first digit for an on-hook</td>
<td></td>
</tr>
<tr>
<td></td>
<td>or off-hook call only.</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>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 &quot;hotline&quot; numbers.</td>
<td>For more information, see the Cisco Unified Communications Manager Administration Guide, &quot;Directory Number Configuration&quot; chapter, &quot;Configuring PLAR&quot; section.</td>
</tr>
</tbody>
</table>
| Privacy | 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. | 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 |
| Programmable Line Keys (PLK) | You 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 "hard" feature. For example, a hard New Call key. | For more information, see:  
- Cisco Unified Communications Manager System Guide, "Cisco Unified IP Phones" chapter  
- Cisco Unified Communications Manager Administration Guide, "Phone Button Template Configuration" chapter  
- Cisco Unified Communications Manager Features and Services Guide, "Modifying Phone Button Templates" chapter |
| Protected Calling | Provides a secure (encrypted) connection between two phones. A security tone plays 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. | For more information about security, see Supported Security Features, on page 12.  
For additional information, see the Cisco Unified Communications Manager Security Guide. |
| Quality Reporting Tool (QRT) | 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. | For more information, see:  
- Cisco Unified Communications Manager System Guide, "Cisco Unified IP Phones" chapter  
- Cisco Unified Communications Manager Features and Services Guide, "Quality Report Tool" chapter |
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Configuration reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redial</td>
<td>Redials the last number dialed on the Cisco Unified IP Phone.</td>
<td>No configuration required.</td>
</tr>
<tr>
<td>Remote Port Configuration</td>
<td>Allows the administrator to configure the speed and duplex functions of the phone Ethernet ports remotely by using Cisco Unified CM Administration. This enhances the performance for large deployments with specific port settings. <strong>Note</strong> If the ports are configured for Remote Port Configuration in Cisco Unified CM, the data cannot be changed on the phone.</td>
<td>To configure the parameter in the Cisco Unified CM Administration application, choose <strong>Device &gt; Phone</strong>, 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 Remote Port Configuration in Enterprise Phone Configuration (<strong>System &gt; Enterprise Phone Configuration</strong>).</td>
</tr>
<tr>
<td>Ring Setting</td>
<td>Identifies the ring type used for a line when a phone has another active call</td>
<td>For more information, see theCisco Unified Communications Manager Administration Guide, &quot;Directory Number Configuration&quot; chapter.</td>
</tr>
<tr>
<td>Ringer Volume Control</td>
<td>The Ringer Volume Control feature enables you 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. The parameter Minimum Ring Volume exists in the Cisco Unified Communications Manager Administration Product Configuration Window. 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 you configure a new minimum volume level after 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 level set by the user. This feature does not apply to handset, speaker, and headset volumes during calls.</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, and scroll to the Product Specific Configuration Layout pane.</td>
</tr>
<tr>
<td>RTCP Hold For SIP</td>
<td>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.</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>
| Secure and Nonsecure          | When a phone is configured as secure (encrypted and trusted) in Cisco Unified CM, it can be given a "protected" status. After that, if desired, the protected phone can be configured to play an indication tone at the beginning of a call: 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. A protected phone plays or does not play a tone under these circumstances:  
  • When the Play Secure Indication Tone option is enabled (True):  
    ◦ 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).  
    ◦ 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).  
  • If the Play Secure Indication Tone option is disabled, no tone is played. | Secure and Nonsecure Indication Tone:  
  • Protected Device: To change the status of a secure phone to protected, check the "Protected Device" check box in Cisco Unified Communications Manager Administration > Device > Phone > Phone Configuration.  
  • Play Secure Indication Tone: To enable the protected phone to play a secure or nonsecure indication tone, set the "Play Secure Indication Tone" to True. (The default is False.) For more information, see Set Up Secure and Nonsecure Indication Tone Feature, on page 117. |
| 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 AdvanceAdhocConference parameter is set. | For more information about security, see Supported Security Features, on page 12. For more information, see:  
  • Cisco Unified Communications Manager System Guide, "Conference Bridges" chapter  
  • Cisco Unified Communications Manager Administration Guide, "Conference Bridge Configuration" chapter  
  • Cisco Unified Communications Manager Security Guide |
<p>| Security Hardening            | Improves the phone firmware security.                                                                                                                                                                       | No configuration required.                                                                                   |</p>
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Configuration reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Services</td>
<td>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.</td>
<td>For more information, see: • <em>Cisco Unified Communications Manager Administration Guide</em>, &quot;Cisco Unified IP Phone Configuration&quot; chapter • <em>Cisco Unified Communications Manager System Guide</em>, &quot;Cisco Unified IP Phone Services&quot; chapter</td>
</tr>
<tr>
<td>Services URL Button</td>
<td>Provides one-touch access to information services.</td>
<td>For more information, see the <em>Cisco Unified Communications Manager Administration Guide</em>.</td>
</tr>
<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 flash simultaneously. After a user answers the call from one of the Cisco Unified 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 may 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 multiple 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;Understanding Directory Numbers&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. 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.</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>Feature</td>
<td>Description</td>
<td>Configuration reference</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Single Button Barge     | Allows users to press a line key to Barge or eBarge into a Remote-in-use call. | 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 |
| Speed Dial              | Dials a specified number that has been previously stored.                   | For more information, see:  
  • *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phones Configuration" chapter.  
  • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones Configuration" chapter. |
| SSH Access              | Allows you to enable or disable the SSH Access setting using the Cisco Unified Communications Manager Administration application. 
  This option indicates whether the phone supports the SSH Access. 
  Settings include:  
  • Enabled  
  • Disabled - default  
  When enabled, it allows the phone to accept the SSH connections. 
  Disabling the SSH server functionality of the phone blocks the SSH access to the phone. | For more information, see *Set Up SSH Access Feature*, on page 118.  
If you set the same parameter in the Common Phone Profile window (*Device > Device Settings > Common Phone Profile*) too, the precedence order of the settings is:  
1  Phone Configuration window settings  
2  Common Phone Profile window settings |
| Time-of-Day Routing     | Restricts access to specified telephony features by time period.            | For more information, see:  
  • *Cisco Unified Communications Manager Administration Guide*, “Time Period Configuration” chapter  
  • *Cisco Unified Communications Manager System Guide*, “Time-of-Day Routing” chapter |
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Configuration reference</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>
| UCR 2008                        | The IP Phones using SCCP support Unified Capabilities Requirements (UCR) 2008 by providing the following functions:  
  • Support for Federal Information Processing Standard (FIPS) 104-2  
  • Support for TVS IPv6  
  • Support for 80-bit SRTCP Tagging  
As an IP Phone administrator, some of these functions require you to set up specific parameters in Cisco Unified Communications Manager Administration. | For more information, see UCR 2008 Setup, on page 130. |
| Voice Messaging System          | Enables callers to leave voice messages if calls are unanswered.             |                                                                                         |
| Video Mode (Cisco Unified IP Phone 7911G only) | Allows a user to select the video display mode for viewing a video conference, depending on the modes configured in the system. | For more information, see:  
  • *Cisco Unified Communications Manager Administration Guide*, "Conference Bridge Configuration" chapter  
  • *Cisco Unified Communications Manager System Guide*, "Understanding Video Telephony" chapter |
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Configuration reference</th>
</tr>
</thead>
</table>
| Video Support (Cisco Unified IP Phone 7911G only) | Enable video support on the phone. | For more information, see:  
  - *Cisco Unified Communications Manager Administration Guide*, "Conference Bridge Configuration" chapter  
  - *Cisco Unified Communications Manager System Guide*, "Understanding Video Telephony" chapter  
  - *Cisco VT Advantage Administration Guide*, "Overview of Cisco VT Advantage" chapter |

**Set Up Enbloc Dialing Feature**

To disable enbloc dialing, perform the following steps:

**Procedure**

- **Step 1** in Cisco Unified Communications Manager Administration, go to Device > Phone.
- **Step 2** On the Phone Configuration window, in the Product Specific Configuration Layout area, uncheck the Enbloc Dialing check box.
- **Step 3** Click Apply Config.
- **Step 4** Click Save.

**Set Up Secure and Nonsecure Indication Tone Feature**

You set this option in *Cisco Unified Communications Manager Administration* > System > Service Parameters.

**Procedure**

- **Step 1** Select the server and then the Unified Communications Manager service.
- **Step 2** In the Service Parameter Configuration window, select the option in the Feature - Secure Tone area.
Set Up SSH Access Feature

To configure the parameters in the Cisco Unified Communications Manager Administration applications, perform the following steps:

**Procedure**

**Step 1** Choose **Device > Phone**.

**Step 2** Select the appropriate IP Phones.

**Step 3** Scroll to the Product Specific Configuration Layout pane.

**Step 4** Select Enable from the SSH Access drop-down list box.

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 33: 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><strong>System &gt; Enterprise Phone Configuration</strong></td>
</tr>
<tr>
<td>Common Phone Profile window</td>
<td><strong>Device &gt; Device Settings &gt; Common Phone Profile</strong></td>
</tr>
<tr>
<td>Phone Configuration window</td>
<td><strong>Device &gt; Phone; Product Specific Configuration area of window</strong></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 Directory Setup

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

• Corporate Directory: Allows a user to look up phone numbers for co-workers.
  
  To support this feature, you must configure corporate directories. See [Corporate Directory Setup, on page 119](#) for more information.

• 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. See [Personal Directory Setup, on page 120](#) for more information.

After the LDAP directory configuration completes, users can use the Corporate Directory service on the Cisco Unified IP Phone to look up users in the corporate 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 (TABSync)

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 206 and Cisco Unified IP Phone Address Book Synchronizer Deployment, on page 206.

**Phone Button Templates**

Phone button templates let you assign features to phone buttons. On the Cisco Unified IP Phones 7906G and 7911G, only the Privacy feature (Private softkey) can be configured on the template.

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.

**Modify Phone Template**

The Cisco Unified Communications Manager Device Settings page contains the phone template.
Procedure

Step 1  Choose Device > Device Settings > Phone Button Template in Cisco Unified Communications Manager Administration.

Step 2  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. See the Cisco Unified Communications Manager Administration Guide and the Cisco Unified Communications Manager System Guide for more information.

Phone Button Template for Personal Address Book or Fast Dials

You can modify a phone button template to associate a service URL with a line button. Doing so enables users to have single-button access to the PAB and Fast Dials. Before you modify the phone button template, you must configure PAB or Fast Dials as an IP phone service.

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
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**

1. **Step 1**  From Cisco Unified Communications Manager Administration, choose **Device > Device Settings > Phone Button Template**.
2. **Step 2**  Click **Find**.
3. **Step 3**  Select the phone model.
4. **Step 4**  Click **Copy**, enter a name for the new template, and then click **Save**. The Phone Button Template Configuration window opens.
5. **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.
6. **Step 6**  Click **Save** to create a new phone button template using the service URL.
7. **Step 7**  Choose **Device > Phone** and open the Phone Configuration window for the phone.
8. **Step 8**  Select the new phone button template from the Phone Button Template drop-down list box.
9. **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 and Standard Feature. 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.

It is recommended that you use the standard softkey template which excludes features already assigned to programmable buttons and limits the feature set to the most commonly used ones. This template reduces the number of softkeys displayed on the phone at one time, eliminating the need for users to press the more softkey. For more information, see Phone Button Templates, on page 120.

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 Cisco Unified Communications Manager System Guide.

Note

The Cisco Unified IP Phones support all softkeys that are configurable in Cisco Unified Communications Manager Administration, except for the following:

- Hold
- Resume

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.
Services Setup

The **Services** button on the Cisco Unified IP Phone gives users access to Cisco Unified IP Phones Services. 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 Cisco Unified CM User Options. 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 **Feature > Cisco Unified IP Phone Services** from Cisco Unified Communications Manager Administration. For more information, see the *Cisco Unified Communications Manager Administration Guide* and *Cisco Unified Communications Manager System Guide*.

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 *Internal Support Web Site*, on page 203 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

Cisco Unified Communications Manager User Addition

Adding users to Cisco Unified Communications Manager allows you to display and maintain information about users such as their directory information and passwords.

**Note**

You can manage password rules for LDAP directory users by configuring password expiration and syntax in the directory server application that is integrated with Cisco Unified Communications Manager. For more information and a list of supported directory servers, see the manual *Installing and Configuring the Cisco Customer Directory Configuration Plugin*, located in [http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_installation_guides_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_installation_guides_list.html).

Users added to Cisco Unified Communications Manager can perform these actions:

- Access the corporate directory and other customized directories from a Cisco Unified IP Phone
- Create a personal directory
- Set up speed dial and 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 > Add a New User from Cisco Unified Communications Manager Administration.

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

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

• To add users in batches, use the Bulk Administration Tool (BAT). 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 User Guide*.

### User Options Web Pages Management

From the User Options web page, users can customize and control several phone features and settings. For detailed information about the User Options web pages, see the *Cisco Unified IP Phone 7906G and 7911G 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 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.

  `https://<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 124).

For additional information, see:

• *Cisco Unified Communications Manager Administration Guide*, "User Group Configuration" chapter

• *Cisco Unified Communications Manager Administration Guide*, "End User Configuration" chapter

• *Cisco Unified Communications Manager System Guide*, "Roles and User Groups" chapter

### 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.

Customize User Options Web Page Display

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

- Show Ring Settings
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 34: EnergyWise Configuration Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Enable Power Save Plus | Selects the schedule of days for which the phone powers off. Select multiple days by pressing and holding the **Control** 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.  
**Caution** 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.  
**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. |
| Phone On Time          | 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. |
| Phone Off Time         | The time of day that the phone powers down for the days selected in the Enable Power Save Plus field. If the Phone On Time and the Phone Off Time 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. |
## Features, Templates, Services, and Users

### EnergyWise Setup on Cisco Unified IP Phone

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Phone Off Idle Timeout**   | 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.                                                                                                                                                                                                                                                   |
| **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.                                                                                                                                                                                                                                          |
| **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.                                                                                                                                                                                                                                         |
This checkbox determines if you will allow the EnergyWise domain controller policy to send power level updates to the phones. The following conditions apply:

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.

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 reapply power or the user wakes the phone.

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

The parameters that support UCR 2008 reside in Cisco Unified Communications Manager Administration. The following table describes the parameters and indicates the procedure to change the setting.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow EnergyWise Overrides</td>
<td>This checkbox 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 reapply power or the user wakes the phone.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• To change the power level on the phone again, EnergyWise must reissue a new power level change command.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> 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.</td>
</tr>
</tbody>
</table>
## Table 35: 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 132</td>
</tr>
<tr>
<td></td>
<td>System &gt; Enterprise Phone Configuration</td>
<td>Set Up UCR 2008 in Enterprise Phone Configuration Window, on page 132</td>
</tr>
<tr>
<td>SSH Access</td>
<td>Device &gt; Phone</td>
<td>Set Up UCR 2008 in Phone Configuration Window, on page 132</td>
</tr>
<tr>
<td></td>
<td>Device &gt; Device Settings Common Phone Profile</td>
<td>Set Up UCR 2008 in Common Phone Profile Configuration Window, on page 132</td>
</tr>
<tr>
<td>Web Access</td>
<td>Device &gt; Phone</td>
<td>Set Up UCR 2008 in Phone Configuration Window, on page 132</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Control Web Page Access, on page 165</td>
</tr>
<tr>
<td>HTTPS Server</td>
<td>Device &gt; Phone</td>
<td>Set Up UCR 2008 in Phone Configuration Window, on page 132</td>
</tr>
<tr>
<td></td>
<td>System &gt; Enterprise Phone Configuration</td>
<td>Set Up UCR 2008 in Enterprise Phone Configuration Window, on page 132</td>
</tr>
<tr>
<td>80-bit SRTCP</td>
<td>Device &gt; Device Settings Common Phone Profile</td>
<td>Set Up UCR 2008 in Common Phone Profile Configuration Window, on page 132</td>
</tr>
<tr>
<td></td>
<td>System &gt; Enterprise Phone Configuration</td>
<td>Set Up UCR 2008 in Enterprise Phone Configuration Window, on page 132</td>
</tr>
<tr>
<td>IP Addressing Mode</td>
<td>Device &gt; Device Settings &gt; Common Device Configuration</td>
<td>Network Configuration Menu, on page 57</td>
</tr>
<tr>
<td>IP Addressing Mode Preference for Signaling</td>
<td>Device &gt; Device Settings &gt; Common Device Configuration</td>
<td>Network Configuration Menu, on page 57</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

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 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 > 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.

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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>System &gt; Enterprise Phone Configuration</strong>.</td>
</tr>
<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
Cisco Unified IP Phone Customization

- Configuration File Customization and Modification, page 135
- Custom Phone Ring Creation, page 136
- Custom Background Images, page 138
- Wideband Codec Setup, page 140

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

| Step 1 | 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 137. |
| Step 2 | 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. |
| Step 3 | Use a text editor to edit the Ringlist.xml file. See Ringlist.xml File Format Requirements, on page 136 for information about how to format this file and for a sample Ringlist.xml file. |
| Step 4 | Save your modifications and close the Ringlist.xml file. |
| Step 5 | 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.) |
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 pressing the Applications Menu button and 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 used by the phone. 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:

/Deskspots/95x34x1

For more information, see the “Software Upgrades” chapter in the Cisco Unified 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 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 is shown 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> - <!-- Please Add Images to the end of the list -->
   <ImageItem Image="TFTP:Desktops/95x34x1/TN-Mountain.png"
                URL="TFTP:Desktops/95x34x1/Mountain.png" /> <ImageItem
       Image="TFTP:Desktops/95x34x1/TN-Ocean.png"
       URL="TFTP:Desktops/95x34x1/Ocean.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 appears on the phone.
- Thumbnail image: Version that appears 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.

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: 95 pixels (width) X 34 pixels (height)
- Thumbnail image: 23 pixels (width) X 8 pixels (height)
- Color palette: For best results, set to monochrome (1-bit) when you create a PNG file.

Set Up Custom Background Image

To configure 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 the PNG File Requirements for Custom Background Images, on page 139.

**Step 2** Upload the new PNG files that you created to the following subdirectory in the TFTP server for the Cisco Unified Communications Manager:

/Desktops/95x34x1

**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 IPT Platform Administration. For more information, see the “Software Upgrades” chapter in Cisco Unified Communications Operating System Administration Guide. If the folder does not exist, the folder gets created and the files get uploaded to the folder.

**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 138 for the location of this file, formatting requirements, and a sample file.

Step 5 Save your modifications and close the List.xml file. 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).

Custom Background Images for Large Font Locales

Phone background images may not display properly when large font locales such as Chinese, Japanese, and Korean are used. To modify a background image for proper display, follow these guidelines:

Use the following file sizes when creating PNG files for the Japanese locale:

- 95x28 (full size image)
- 23x8 (thumbnail image)

Upload the image files to %TFTPPATH%/Desktops/95x28x1.

Modify or create the List.xml file in the %TFTPPATH%/Desktops/95x28x1 folder to include the following lines, where image.png is the name of your image file:

```xml
<CiscoIPPhoneImageList>
<ImageItemImage="TFTP:Desktops/95x28x1/image.png" URL="TFTP:Desktops/95x28x1/image.png" />  
</CiscoIPPhoneImageList>
```

For more information, see Custom Background Images, on page 138.

Wideband Codec Setup

If Cisco Unified Communications Manager has been configured to use G.722 and if the far endpoint supports G.722, the call can connect using the G.722 codec in place of G.711. 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 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 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, choose System > Enterprise Parameters. The default value of this enterprise parameter is True, which means that all Cisco Unified IP Phone Models 7906G and 7911G that are registered to this Cisco Unified Communications Manager...
will advertise G.722 to Cisco Unified Communications Manager. For more information, see Cisco Unified Communications Manager System Guide, "Cisco Unified IP Phones" chapter.

- Advertise G.722 Codec: From Cisco Unified Communications Manager, 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 Advertise G.722 Codec parameter on the Product Specific Configuration area of the Phone Configuration window.
Model Information, Status, and Statistics

- Model Information, Status, and Statistics Overview, page 143
- Display Model Information Screen, page 143
- Status Menu, page 145
- Test Tone, page 160

Model Information, Status, and Statistics Overview

This chapter describes how to use the following menus on the Cisco Unified IP Phones 7906G and 7911G 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.

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's web page. For more information, see Remote Monitoring, on page 163.

For more information about troubleshooting the Cisco Unified IP Phone 7906G and 7911G, see Troubleshooting and Maintenance, on page 179.

Display Model Information Screen

The Model Information screen displays specific information about the IP phone. To display the Model Information screen, perform these steps:
**Procedure**

**Step 1** Press **Applications Menu**.

**Step 2** Select **Settings > Model Information**.

The Model information screen includes the options described in [Model Information Fields](#), on page 144.

---

### Model Information Fields

The following table describes the Model Information fields.

**Table 36: 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 (used for the</td>
<td>For information about how to manage the MIC for a</td>
</tr>
<tr>
<td></td>
<td>security features) is installed on the phone (Yes) or is not installed on</td>
<td>phone, see the &quot;Using the Certificate Authority</td>
</tr>
<tr>
<td></td>
<td>the phone (No).</td>
<td>Proxy Function&quot; chapter in <em>Cisco Unified Communications Manager Security Guide</em>.</td>
</tr>
<tr>
<td>LSC</td>
<td>Indicates whether a locally significant certificate (used for the security</td>
<td>For information about how to manage the MIC for a</td>
</tr>
<tr>
<td></td>
<td>features) is installed on the phone (Yes) or is not installed on the phone</td>
<td>phone, see the &quot;Using the Certificate Authority</td>
</tr>
<tr>
<td></td>
<td>(No)</td>
<td>Proxy Function&quot; chapter in <em>Cisco Unified Communications Manager Security Guide</em>.</td>
</tr>
<tr>
<td>Call Control Protocol</td>
<td>Displays the call control protocol for the phone,</td>
<td>See <a href="#">Cisco Unified IP Phones and Different Protocols</a>, on page 36.</td>
</tr>
<tr>
<td></td>
<td>Skinny Client Control Protocol (SCCP).</td>
<td></td>
</tr>
</tbody>
</table>

---

_Cisco Unified IP Phone 7906G and 7911G Administration Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)_; 144
Status Menu

The following table provides a list of Status menu options and a description of each option.

Table 37: Status Messages

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status Messages</td>
<td>Displays the Status Messages screen, which shows a log of important system messages. For more information, see Status Messages Screen, on page 145.</td>
</tr>
<tr>
<td>Network Statistics</td>
<td>Displays the Network Statistics screen, which shows Ethernet traffic statistics. For more information, see Network Statistics Screen, on page 152.</td>
</tr>
<tr>
<td>Firmware Versions</td>
<td>Displays the Firmware Versions screen, which shows information about the firmware running on the phone. For more information, see Firmware Versions Screen, on page 156.</td>
</tr>
<tr>
<td>802.1X Authentication Status</td>
<td>Displays the time-stamped authentication successes and failures. For more information, see Call Statistics Screen, on page 157.</td>
</tr>
</tbody>
</table>

Display Status Menu

**Procedure**

**Step 1**
Press Apps.

**Step 2**
Select Admin Settings > Status Menu.

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. Status Messages, on page 146 describes the status messages that might appear. This table also includes actions you can take to address errors.

Display Status Messages Screen

To display the Status Messages screen, perform these steps:
Procedure

Step 1 Press Applications Menu.
Step 2 Select Settings.
Step 3 Select Status.
Step 4 Select Status Messages.
Step 5 To remove current status messages, press the Clear.
Step 6 To exit the Status Messages screen, press the Exit.

Status Messages

The following table describes the status messages.

Table 38: Status Messages

<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 from 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>The Cisco Unified Configuration Manager creates a configuration file for the phone when 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>
<tr>
<td>CFG TFTP Size Error</td>
<td>The configuration file is too large for file system on the phone.</td>
<td>Power cycle the phone.</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>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 installed</td>
<td>The CTL file is installed in 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>
<tr>
<td>CTL and ITL installed</td>
<td>The CTL and ITL files are installed on the phone.</td>
<td>None. This message is informational only. Phone does not have prior installation of either CTL or ITL file. 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 57 for details on assigning a static IP address. |
| Disabled             | 802.1X Authentication is disabled on the phone. | You can enable 802.1X using the Settings > Security Configuration > 802.1X Authentication option on the phone. For more information, see 802.1X Authentication and Status, on page 94. |
| DNS timeout          | DNS server did not respond.         | • 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. |
| DNS unknown host     | DNS could not resolve the name of the TFTP server or Cisco Unified Communications Manager. | • 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. |
<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
<th>Possible explanation and action</th>
</tr>
</thead>
<tbody>
<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 57 for details.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 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>
<tr>
<td>Error update locale</td>
<td>One or more localization files could not be found in the tftp directory or were not valid. The locale was not changed.</td>
<td>From Cisco Unified Operating System Administration, check that the following files are located within subdirectories in the TFTP File Management:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Located in subdirectory with same name as network locale:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>* tones.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Located in subdirectory with same name as user locale:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>* glyphs.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td>* dictionary.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td>* kate.xml</td>
</tr>
<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>Message</td>
<td>Description</td>
<td>Possible explanation and action</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</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 using Cisco Unified Communications Manager Administration. Then add the phone back to the Cisco Unified Communications Manager database using Cisco Unified Communications Manager Administration.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• There is a problem with the CTL file 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 is specified in the phone configuration file.</td>
<td>From Cisco Unified Operating System Administration, make sure that the phone load file is on the TFTP server, and that the entry in the configuration file is correct.</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 57 for details.</td>
</tr>
<tr>
<td>ITL installed</td>
<td>The ITL file is installed in the phone.</td>
<td>None. This message is informational only. The ITL file was not installed previously. For more information about the CTL file, see the Cisco Unified Communications Manager Security Guide.</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>Load rejected HC</td>
<td>The application that was downloaded is not compatible with the phone's 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 Firmware Versions Screen, on page 156 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 Network Configuration Menu, on page 57 for details.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 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 Network Configuration Menu, on page 57 for details.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 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 CTL file or the ITL file is not installed on the phone.</td>
<td>The Trust List is not configured on the Cisco Unified Communications Manager, which does not support security by default. For more information about CTL and ITL files, see the Cisco Unified Communications Manager Security Guide.</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>Message</td>
<td>Description</td>
<td>Possible explanation and action</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------</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 is pointing to the correct TFTP server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If you are using static IP addresses, check configuration of TFTP server. See Network Configuration Menu, on page 57 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• No network connectivity between the TFTP server and the phone: Verify the network connections.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 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 to the absence of an authenticator.</td>
<td>Authentication typically times out if 802.1X is not configured on the switch.</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. For more information about the Trust List, see the Cisco Unified Communications Manager Security Guide.</td>
</tr>
</tbody>
</table>
The CTL and ITL files are installed on the phone, and it failed to update the new files. Possible reasons for failure:

- Network failure
- TFTP server was down
- 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
- Internal phone failure

Possible solutions:

- Check the network connectivity
- Check if the TFTP server is active and functioning normally
- If the TVS server is supported on Cisco Unified Communications Manager, check if the TVS server is active and functioning normally
- Verify if the security token and the TFTP server are valid
- Manually delete the CTL and ITL files if all the above solutions fail, and reset the phone.

<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
<th>Possible explanation and action</th>
</tr>
</thead>
</table>
| Trust List update failed             | Updating CTL file and ITL failed.                | The CTL and ITL files are installed on the phone, and it failed to update the new files. Possible reasons for failure:  
  • Network failure  
  • TFTP server was down  
  • 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  
  • Internal phone failure  
  Possible solutions:  
  • Check the network connectivity  
  • Check if the TFTP server is active and functioning normally  
  • If the TVS server is supported on Cisco Unified Communications Manager, check if the TVS server is active and functioning normally  
  • Verify if the security token and the TFTP server are valid  
  • Manually delete the CTL and ITL files if all the above solutions fail, and reset the phone. |
| Version error                        | The name of the phone load file is incorrect.    | Make sure that the phone load file has the correct name.                                        |
| XmlDefault corresponding to the phone device name | Name of the configuration file.                  | None. This is an informational message indicating the name of the configuration file for the phone. |

**Network Statistics Screen**

The Network Statistics screen displays information about the phone and network performance. [Network Statistics Items, on page 153](#) provides a list of Network Statistics items and a description of each item.

**Display Network Statistics Screen**

To display the Network Statistics screen, perform these steps:
Procedure

**Step 1**  Press **Applications**.
**Step 2**  Select **Settings**.
**Step 3**  Select **Status**.
**Step 4**  Select **Network Statistics**.
**Step 5**  To reset the Rx Frames, Tx Frames, and Rx Broadcasts statistics to 0, press **Clear**.

Network Statistics Items

The following table describes the Network Statistics items.

**Table 39: 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>
</tbody>
</table>
| One of the following values:  
  • Initialized  
  • TCP-timeout  
  • CM-closed-TCP  
  • TCP-Bad-ACK  
  • CM-reset-TCP  
  • CM-aborted-TCP  
  • CM-NAKed  
  • KeepaliveTO  
  • Failback  
  • Phone-Keypad  
  • Phone-Re-IP  
  • Reset-Reset  
  • Reset-Restart  
  • Phone-Reg-Rej  
  • Load Rejected HC  
  • CM-ICMP-Unreach  
  • Phone-Abort | Cause of the last phone reset |
<p>| Elapsed Time | Amount of time that has elapsed since the phone connected to Cisco Unified Communications Manager |
| Port 1 | Link state and connection of the Network port |
| Port 2 (applies to 7911G only) | 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. |</p>
<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4</td>
<td>Information on the DHCP status. This includes the following states:</td>
</tr>
<tr>
<td></td>
<td>• CDP BOUND</td>
</tr>
<tr>
<td></td>
<td>• CDP INIT</td>
</tr>
<tr>
<td></td>
<td>• DHCP BOUND</td>
</tr>
<tr>
<td></td>
<td>• DHCP DISABLED</td>
</tr>
<tr>
<td></td>
<td>• DHCP INIT</td>
</tr>
<tr>
<td></td>
<td>• DHCP INVALID</td>
</tr>
<tr>
<td></td>
<td>• DHCP REBINDING</td>
</tr>
<tr>
<td></td>
<td>• DHCP REBOOT</td>
</tr>
<tr>
<td></td>
<td>• DHCP RENEWING</td>
</tr>
<tr>
<td></td>
<td>• DHCP REQUESTING</td>
</tr>
<tr>
<td></td>
<td>• DHCP RESYNC</td>
</tr>
<tr>
<td></td>
<td>• DHCP UNRECOGNIZED</td>
</tr>
<tr>
<td></td>
<td>• DHCP WAITING COLDBOOT TIMEOUT</td>
</tr>
<tr>
<td></td>
<td>• SET DHCP COLDBOOT</td>
</tr>
<tr>
<td></td>
<td>• SET DHCP DISABLED</td>
</tr>
<tr>
<td></td>
<td>• DISABLED DUPLICATE IP</td>
</tr>
<tr>
<td></td>
<td>• SET DHCP FAST</td>
</tr>
<tr>
<td>^-</td>
<td>Description</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<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 Versions Screen**

The Firmware Versions screen displays information about the firmware version running on the phone.

**Display Firmware Versions Screen**

To display the Firmware Version screen, perform these steps:
**Procedure**

**Step 1** Press *Applications Menu*.

**Step 2** Select *Settings > Status*.

**Step 3** Select *Firmware Versions*.

**Step 4** To exit the Firmware Version screen, press *Exit*.

---

**Firmware Version Fields**

The following table provides a list of Firmware Version items and a description of each field.

<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>Identifies the JAR file running on the phone</td>
</tr>
<tr>
<td>JVM Load ID</td>
<td>Identifies the Java Virtual Machine (JVM) running on the phone</td>
</tr>
<tr>
<td>OS Load ID</td>
<td>Identifies the operating system running on the phone</td>
</tr>
<tr>
<td>Boot Load ID</td>
<td>Identifies the factory-installed load running on the phone</td>
</tr>
<tr>
<td>DSP Load ID</td>
<td>Identifies the DSP load file running on the phone.</td>
</tr>
</tbody>
</table>

---

**Call Statistics Screen**

You can access the Call Statistics screen on the phone to display counters, statistics, and voice-quality metrics. After a call, you can view the call information captured during the last call by displaying the Call Statistics screen.

---

**Note**

You can 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 that are not available on the phone. For more information about remote monitoring, see *Streaming Statistics*, on page 175.

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, perform these steps:

**Procedure**

**Step 1** Press **Settings**.
**Step 2** Select **Status**.
**Step 3** Select **Call Statistics**.

Call Statistics Fields

The Call Statistics screen displays these items:

**Table 41: Call Statistics Items**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revr Codec</td>
<td>Type of voice stream received (RTP streaming audio from codec): G.729, G.728/iLBC, G.711 u-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 u-law, G.711 A-law, or Lin16k.</td>
</tr>
<tr>
<td>Revr 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>Revr Packets</td>
<td>Number of RTP voice packets received since voice stream was opened.</td>
</tr>
<tr>
<td>Sender Packets</td>
<td>Number of RTP voice packets transmitted since voice stream was opened.</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 was opened.</td>
</tr>
</tbody>
</table>
**Item** | **Description**
---|---
Max Jitter | Maximum jitter observed since the receiving voice stream was opened.
Rcvr Discarded | Number of RTP packets in the receiving voice stream that have been discarded (bad packets, too late, and so on).
**Note** | The phone discards payload type 19 comfort noise packets that are generated by Cisco Gateways, which will increment this counter.
Rcvr Lost Packets | Missing RTP packets (lost in transit).

**Voice Quality Metrics**

**MOS LQK** | 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 199.
**Note** | The MOS LQK score can vary based on the type of codec that the Cisco Unified IP Phone uses.
Avg MOS LQK | Average MOS LQK score observed for the entire voice stream.
Min MOS LQK | Lowest MOS LQK score observed from start of the voice stream.
Max MOS LQK | 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:
- G.711 gives 4.5
- G.722 gives 4.5
- G.728/ilBC gives 3.9
- G.729 A/AB gives 3.8
MOS LQK Version | Version of the Cisco proprietary algorithm used to calculate MOS LQK scores.
Cumulative Conceal Ratio | Total number of concealment frames divided by total number of speech frames received from start of the voice stream.
Interval Conceal Ratio | 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.
Max Conceal Ratio | Highest interval concealment ratio from start of the voice stream.
### Item Description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 below)</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 161.

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

- Remote Monitoring Overview, page 163
- Access Web Page for Phone, page 164
- Phone Web Page Overview, page 164
- Control Web Page Access, page 165
- Device Information Area, page 166
- Network Configuration Area, page 167
- Network Statistics Area, page 171
- Device Logs Area, page 174
- Streaming Statistics, page 175

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

Note

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 143.

For more information about troubleshooting the Cisco Unified IP Phone 7906G and 7911G, see Troubleshooting and Maintenance, on page 179.

Access Web Page for Phone

To access the web page for a Cisco Unified IP Phone, perform the following these steps.

**Note**

If you cannot access the web page, it may be disabled. See Control Web Page Access, on page 165 for more information.

**Procedure**

**Step 1** Obtain the IP address of the Cisco Unified IP Phone using one of these methods:

- 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.
- On the phone, press the Applications Menu 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)

Phone Web Page Overview

The web page for 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**: Displays up to the 10 most recent status messages that the phone has generated since it was last powered up.

• **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**, and **Stream 3** hyperlinks, which display a variety of streaming statistics.

**Related Topics**

- Device Information Area, on page 166
- Network Configuration Area, on page 167
- Network Statistics Area, on page 171
- Device Logs Area, on page 174
- Streaming Statistics, on page 175

---

**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 User Options web pages of the phone.

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, perform 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** From the Web Access drop-down list box, choose **Disable** if you want to disable the phone and choose **Enabled** if you want to enable the phone.

**Step 5** Click **Update**.
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 phones 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 the Access Web Page for Phone, on page 164, and then click the **Device Information** hyperlink.

**Table 42: 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 the 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>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>
</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 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
Timezone 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

---

### 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 these items.

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 97.

To display the Network Configuration area, access the web page for the phone as described in the Access Web Page for Phone, on page 164, 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>Item</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</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 1–5</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 1–5</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>
</tbody>
</table>
| Unified CM1–5      | 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 option may also include the Survivable Remote Site Telephony (SRST) designation, which indicates 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. |
<p>| Information URL    | URL of the help text that appears on the phone.                                                                                                                                                             |</p>
<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directories URL</td>
<td>URL of the server from which the phone obtains directory information.</td>
</tr>
<tr>
<td>Messages URL</td>
<td>URL of the server from which the phone obtains message services.</td>
</tr>
<tr>
<td>Services URL</td>
<td>URL of the server from which the phone obtains Cisco Unified IP Phone services.</td>
</tr>
<tr>
<td>DHCP Enabled</td>
<td>Indicates whether DHCP is being used by the phone.</td>
</tr>
<tr>
<td>DHCP Address Released</td>
<td>Indicates the setting of the DHCP Address Released option on the phone’s Network Configuration menu.</td>
</tr>
<tr>
<td>Alternate TFTP</td>
<td>Indicates whether the phone is using an alternative TFTP server.</td>
</tr>
<tr>
<td>Idle URL</td>
<td>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.</td>
</tr>
<tr>
<td>Idle URL Time</td>
<td>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.</td>
</tr>
<tr>
<td>Proxy Server URL</td>
<td>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.</td>
</tr>
<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>• No Link: No connection to the switch port</td>
</tr>
</tbody>
</table>
### PC Port Configuration (applies to 7911G only)

Speed and duplex of the switch port, where:
- **A**: Auto Negotiate
- **10H**: 10-BaseT/half duplex
- **10F**: 10-BaseT/full duplex
- **100H**: 100-BaseT/half duplex
- **100F**: 100-BaseT/full duplex
- **No Link**: No connection to the PC port

To configure the setting on multiple phones simultaneously, configure Remote Port Configuration in Enterprise Phone Configuration (System &gt; 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>PC Port Configuration (applies to 7911G only)</td>
<td>Speed and duplex of the switch port, where:</td>
</tr>
<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 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 definitions of the tones and cadences used by the phone.</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 (applies to 7911G only)</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>Group Listen</td>
<td>Enables both the handset and speaker to be active at the same time, so that one user can talk into the handset while other users listen over the speaker.</td>
</tr>
<tr>
<td>GARP Enabled</td>
<td>Indicates whether the phone learns MAC addresses from GARP responses.</td>
</tr>
<tr>
<td>Voice VLAN Enabled (applies to 7911G only)</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 Enabled</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>
</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. [Ethernet Information Area Fields, on page 172](#) describes the items in this area.
- **Access area:** Displays information about network traffic to and from the PC port on the phone. [Access and Network Area Fields, on page 172](#) describes the items in this area.
- **Network area:** Displays information about network traffic to and from the network port on the phone. [Access and Network Area Fields, on page 172](#) describes the items in this area.

### Table of Network Statistics

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 (applies to 7911G only)</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 (applies to 7911G only)</td>
<td>VLAN used to identify and remove 802.1P/Q tags from packets sent to the PC.</td>
</tr>
<tr>
<td>CDP: PC Port (applies to 7911G only)</td>
<td>Indicates whether CDP is enabled on the PC port (default is enabled).</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-MED: SW Port</td>
<td>Indicates whether Link Layer Discovery Protocol Media Endpoint Discovery (LLDP-MED) is enabled on the switch port.</td>
</tr>
</tbody>
</table>
| LLDP Power Priority | 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 |
| LLDP Asset ID | Identifies the asset ID assigned to the phone for inventory management. |
| SSH Access Enabled | Indicates whether the phone accepts or blocks the SSH connections. |
To display a network statistics area, access the web page for the phone as described in the Access Web Page for Phone, on page 164, and then click the Ethernet Information, the Access, and or the Network hyperlink.

**Ethernet Information Area Fields**

*Table 44: 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 transmitted by the phone</td>
</tr>
<tr>
<td>Tx broadcast</td>
<td>Total number of broadcast packets transmitted by the phone</td>
</tr>
<tr>
<td>Tx multicast</td>
<td>Total number of multicast packets transmitted by the phone</td>
</tr>
<tr>
<td>Tx unicast</td>
<td>Total number of unicast packets transmitted by the phone</td>
</tr>
<tr>
<td>Rx Frames</td>
<td>Total number of packets received by the phone</td>
</tr>
<tr>
<td>Rx broadcast</td>
<td>Total number of broadcast packets received by the phone</td>
</tr>
<tr>
<td>Rx multicast</td>
<td>Total number of multicast packets received by the phone</td>
</tr>
<tr>
<td>Rx unicast</td>
<td>Total number of unicast packets received by the phone</td>
</tr>
<tr>
<td>RxPacketNoDes</td>
<td>Total number of shed packets caused by no direct memory access (DMA) descriptor</td>
</tr>
</tbody>
</table>

**Access and Network Area Fields**

*Table 45: Access Area and Network Area Items*

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rx totalPkt</td>
<td>Total number of packets received by the phone</td>
</tr>
<tr>
<td>Rx crcErr</td>
<td>Total number of packets received with CRC failed</td>
</tr>
<tr>
<td>Rx alignErr</td>
<td>Total number of packets received between 64 and 1522 bytes in length that have a bad Frame Check Sequence (FCS)</td>
</tr>
<tr>
<td>Rx multicast</td>
<td>Total number of multicast packets received by the phone</td>
</tr>
<tr>
<td>Rx broadcast</td>
<td>Total number of broadcast packets received by the phone</td>
</tr>
<tr>
<td>Rx unicast</td>
<td>Total number of unicast packets received by the phone</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Rx shortErr</td>
<td>Total number of frame check sequence (FCS) error packets or Align error packets received that are less than 64 bytes in size</td>
</tr>
<tr>
<td>Rx shortGood</td>
<td>Total number of good packets received that are less than 64 bytes size</td>
</tr>
<tr>
<td>Rx longGood</td>
<td>Total number of good packets received that 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 received 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 received, including bad packets, that are between 65 and 127 bytes in size</td>
</tr>
<tr>
<td>Rx size128to255</td>
<td>Total number of packets received, including bad packets, that are between 128 and 255 bytes in size</td>
</tr>
<tr>
<td>Rx size256to511</td>
<td>Total number of packets received, including bad packets, that are between 256 and 511 bytes in size</td>
</tr>
<tr>
<td>Rx size512to1023</td>
<td>Total number of packets received, including bad packets, that are between 512 and 1023 bytes in size</td>
</tr>
<tr>
<td>Rx size1024to1518</td>
<td>Total number of packets received, 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) received by the phone</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 transmitted by the phone</td>
</tr>
<tr>
<td>Tx multicast</td>
<td>Total number of multicast packets transmitted by the phone</td>
</tr>
<tr>
<td>LLDP FramesOutTotal</td>
<td>Total number of LLDP frames sent out from the phone</td>
</tr>
</tbody>
</table>
### Device Logs Area

The Device Logs area on a phone web page provides information 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, on page 146 describes the status messages that can appear.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 received on the phone.</td>
</tr>
<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 the Status Messages, access the web page for the phone as described in the Access Web Page for Phone, on page 164, 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 stream. For example, a barged call uses Stream 1 and Stream 2.

To display a Streaming Statistics area, access the web page for the phone as described in the Access Web Page for Phone, on page 164, and then click the Stream 1, the Stream 2, or the Stream 3 hyperlink.

The following table describes the items in the Streaming Statistics areas.

<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 (see note)</td>
<td>Number of times the RTCP Sender Reports have been sent.</td>
</tr>
<tr>
<td>Sender Report Time Sent (see note)</td>
<td>Internal time stamp indication when a RTCP Sender Report was sent.</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Recvr 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>Recvr Codec</td>
<td>Type of audio encoding used for the received stream.</td>
</tr>
<tr>
<td>Recvr 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>Recvr Report Time Sent(see note)</td>
<td>Internal time stamp indication when a RTCP Receiver Report was sent.</td>
</tr>
<tr>
<td>Recvr Packets</td>
<td>Total number of RTP data packets received by the phone since starting receiving data on this connection. Includes packets received from different sources if this is a multicast call. The value displays as 0 if the connection was set to send-only mode.</td>
</tr>
<tr>
<td>Recvr Octets</td>
<td>Total number of payload octets received in RTP data packets by the device since starting reception on the connection. Includes packets received from different sources if this is a multicast call. The value displays as 0 if 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 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 199. The MOS LQK score can vary based on the type of codec that the Cisco Unified IP Phone uses.</td>
</tr>
<tr>
<td>Note</td>
<td></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.729 A /AB gives 3.8</td>
</tr>
<tr>
<td></td>
<td>• G.728/I LBC gives 3.9</td>
</tr>
</tbody>
</table>

Note: MOS LQK scores 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 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</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>of active speech. If using voice activity detection (VAD), a longer interval</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>running average of the round-trip delay, measured when RTCP receiver report</td>
</tr>
<tr>
<td></td>
<td>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</td>
<td>Number of times RTCP Sender Reports have been received.</td>
</tr>
<tr>
<td>(see note)</td>
<td></td>
</tr>
<tr>
<td>Sender Report Time Received</td>
<td>Last time at which an RTCP Sender Report was received.</td>
</tr>
<tr>
<td>(see note)</td>
<td></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</td>
<td>Number of times RTCP Receiver Reports have been received.</td>
</tr>
<tr>
<td>(see note)</td>
<td></td>
</tr>
<tr>
<td>Rcvr Report Time Received</td>
<td>Last time at which an RTCP Receiver Report was received.</td>
</tr>
<tr>
<td>(see note)</td>
<td></td>
</tr>
<tr>
<td>Voice Quality Metrics</td>
<td></td>
</tr>
</tbody>
</table>
### Description

- **MOS LQK**: 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 199. The MOS LQK score can vary based on the type of codec that the Cisco Unified IP Phone uses.

### Item | Description
---|---
MOS LQK | 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 199. The MOS LQK score can vary based on the type of codec that the Cisco Unified IP Phone uses.

- **Avg MOS LQK**: Average MOS LQK score observed for the entire voice stream.
- **Min MOS LQK**: Lowest MOS LQK score observed from start of the voice stream.
- **Max MOS LQK**: 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:
  - G.711 gives 4.5
  - G.729 A /AB gives 3.7
- **MOS LQK Version**: Version of the Cisco proprietary algorithm used to calculate MOS LQK scores.
- **Cmltve Conceal Ratio**: Total number of concealment frames divided by total number of speech frames received from start of the voice stream.
- **Interval Conceal Ratio**: 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.
- **Max Conceal Ratio**: Highest interval concealment ratio from start of the voice stream.
- **Conceal Secs**: Number of seconds that have concealment events (lost frames) from the start of the voice stream (includes severely concealed seconds).
- **Severely Conceal Secs**: Number of seconds that have more than 5 percent concealment events (lost frames) from the start of the voice stream.

---

**Note**

When the RTP Control Protocol is disabled, no data generates for this field, so it displays as 0.

**Related Topics**

- [Cisco Unified IP Phone Settings](#), on page 53
- [Features, Templates, Services, and Users](#), on page 97
- [Call Statistics Screen](#), on page 157
- [Voice Quality Monitoring](#), on page 199
Troubleshooting and Maintenance

- Troubleshooting and Maintenance Overview, page 179
- Troubleshooting, page 179
- Maintenance, page 199

Troubleshooting and Maintenance Overview

This chapter provides information that can assist you in troubleshooting problems with your Cisco Unified IP Phone 7906G or 7911G or with your Cisco Unified Communications 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, available to registered Cisco.com users at this URL:


Troubleshooting

This section contains 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 the Phone Startup Verification, on page 50. 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 its 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, lack of power, and so on. Or, the phone may not be functional.

Solution
To determine whether the phone is functional, 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.
   - Disconnect a functioning Cisco Unified IP Phone from another port and connect it to this network port to verify the port is active.
   - Connect the Cisco Unified IP Phone that will not start up to a different network port that is known to be good.
   - Connect the Cisco Unified IP Phone that will not start up 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, use the external power supply instead.
   - If you are using the external power supply, switch with a unit that you know to be functional.

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. For instructions, see Perform Factory Reset, on page 198.

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.

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 145 for instructions about accessing status messages and for a list of potential errors, their explanations, and their solutions.

Cisco Unified Communications Manager Phone Registration

Problem
The phone is not registered with the 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 the Cisco Unified Communications Manager Phone Addition Methods, on page 33 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 > Find from Cisco Unified Communications Manager Administration to search for the phone based on its MAC Address. For information about determining a MAC address, see Cisco Unified IP Phone MAC Address Determination, on page 37.

If the phone is already in the Cisco Unified Communications Manager database, its configuration file may be damaged. See Create New Configuration File, on page 194 for assistance.

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 192.
### IP Address 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 193.

### 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 193.

### Cisco Unified Communications Manager Settings on Phone

**Problem**
The phone may not have the correct information about the Cisco Unified Communications Manager.

**Solution**
On the Cisco Unified IP Phone, press the **Applications Menu** button and select **Settings > Network Configuration > Communications Manager 1–5**. 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 181 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 193.

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 Configuration File, on page 194

Cisco Unified Communications Manager Phone Registration

Problem
The phone is not registered with the 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 the Cisco Unified Communications Manager Phone Addition Methods, on page 33 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 its MAC Address. For information about determining a MAC address, see Cisco Unified IP Phone MAC Address Determination, on page 37.

If the phone is already in the Cisco Unified Communications Manager database, its configuration file may be damaged. See Create New Configuration File, on page 194 for assistance.

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 some encryption functionality to be existing. 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, try 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 Perform Factory Reset, on page 198.

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. See Network Configuration Menu, on page 57 for more information.
2. Verify that the DHCP server has been set up properly.
3. Verify the DHCP lease duration. Cisco recommends that you set the lease duration to 8 days. Cisco Unified IP Phones send messages with request type 151 to renew their DHCP address leases. If the DHCP server expects messages with request type 150, the lease renewal is denied, forcing the phone 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 195.

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 describe problems with the CTL file:
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.

CTL File Authenticates but Other Configuration Files Do Not Authenticate

**Problem**
Phone cannot authenticate any configuration files other than the CTL file.

**Cause**
A bad TFTP record exists, or the configuration file may not be signed by the corresponding certificate in the phone Trust List.

**Solution**
Check the TFTP record and the certificate in the Trust List.

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 47: 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 189</td>
</tr>
<tr>
<td>• Phone does not register with Cisco Unified Communications Manager.</td>
<td></td>
</tr>
<tr>
<td>• 802.1X Authentication Status displays as &quot;Held&quot; (see 802.1X Authentication and Status, on page 94).</td>
<td></td>
</tr>
<tr>
<td>• Status menu displays 802.1X status as &quot;Failed&quot; (see Status Menu, on page 145)</td>
<td></td>
</tr>
</tbody>
</table>
If all the following conditions apply, See

<table>
<thead>
<tr>
<th>Condition</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Phone cannot obtain a DHCP-assigned IP address.</td>
<td>802.1X Not Enabled, on page 190</td>
</tr>
<tr>
<td>• Phone does not register with Cisco Unified Communications Manager.</td>
<td></td>
</tr>
<tr>
<td>• Phone status display as &quot;Configuring IP&quot; or &quot;Registering&quot;.</td>
<td></td>
</tr>
<tr>
<td>• 802.1X Authentication Status displays as &quot;Disabled&quot;.</td>
<td></td>
</tr>
<tr>
<td>• Status menu displays DHCP status as timing out.</td>
<td></td>
</tr>
<tr>
<td>• Phone cannot obtain a DHCP-assigned IP address.</td>
<td>Factory Reset of Phone Has Deleted 802.1X Shared Secret, on page 190</td>
</tr>
<tr>
<td>• Phone does not register with Cisco Unified Communications Manager.</td>
<td></td>
</tr>
<tr>
<td>• Phone status display as &quot;Configuring IP&quot; or &quot;Registering.&quot;</td>
<td></td>
</tr>
<tr>
<td>• Cannot access phone menus to verify 802.1X status.</td>
<td></td>
</tr>
</tbody>
</table>

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.

Solution
1. Verify that you have properly configured the required components (see 802.1X Authentication, on page 18 for more information).
2. Confirm that the shared secret is configured on the phone. See 802.1X Authentication and Status, on page 94 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 shared secret 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 is not enabled on the phone.

**Solution**
To enable 802.1X, see Security Configuration Menu, on page 80.

**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 completed a factory reset (see Perform Factory Reset, on page 198) 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 issue, you have two options:

• Temporarily disable 802.1X on the switch
• Temporarily move the phone to a network environment that is not using 802.1X authentication

After 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, on page 94).

**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.

Poor Audio Quality With Calls That Route Outside Cisco Unified Communications Manager

Problem
Poor quality with tandem audio encoding. Tandem encoding can occur when making calls between an IP Phone and a digital cellular phone, when using a conference bridge, or in situations where IP to IP calls are partially routed across the PSTN.

Cause
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 digital cellular phone will have poor voice quality.

Solution
Use the G.729 codec only when absolutely necessary.

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

The following sections help troubleshoot general telephone call problems.

Phone Call Cannot Be Established

Problem
A user complains about not being able to make a call.
Cause
The phone does not have a DHCP IP address, is unable to register to Cisco Unified Communications Manager. Phones with an LCD display show the message Configuring IP or Registering. Phones without an LCD display play the reorder tone (instead of dial tone) in the handset when the user attempts to make a call.

Solution
1  Verify the following:
   a  The Ethernet cable is attached.
   b  The Cisco CallManager service is running on the Cisco Unified Communications Manager server.
   c  Both phones are registered to the same Cisco Unified Communications Manager.

2  Audio server debug and capture logs are enabled for both phones. If needed, enable Java debug.

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.

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 IPv4 > Network Configuration, 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 57.

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 57 for instructions.
Check DHCP settings

Procedure

Step 1  On the Cisco Unified IP Phone, press Applications Menu, then select Settings > Network Configuration, and look at the following options:
  a) 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. For more information, see Troubleshooting Switch Port Problems, available at this URL: http://www.cisco.com/en/US/customer/products/hw/switches/ps708/prod_tech_notes_list.html
  b) 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 57 for instructions.

Step 2  If you are using DHCP, check the IP addresses distributed by your DHCP server. For more information, see Understanding and Troubleshooting DHCP in Catalyst Switch or Enterprise Networks, available 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  Press Applications Menu.
Step 2  Select Settings > Network Configuration > DNS Server 1.
Step 3  You should also verify that there is a CNAME entry in the DNS server for the TFTP server and for the Cisco Unified Communications Manager system.
Step 4  You must also ensure that DNS is configured to do reverse look-ups. Windows 2000 is configured by default only to perform forward look-ups.

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.

Create New Configuration File

**Note**

- When you remove a phone from the Cisco Unified Communications Manager database, its 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. For more information, see the **Cisco Unified Communications Manager Administration Guide**.

- 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 there is no button on the phone 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, perform 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 33 for details.

Step 4 Power cycle the phone.
Determine DNS or Connectivity Issues

If the phone continues to reset, follow these steps to eliminate DNS or other connectivity errors:

Procedure

**Step 1** Use the **Erase** softkey to reset phone settings to their default values. See [Cisco Unified IP Phone Reset or Restore](#) on page 197 for details.

**Step 2** Modify DHCP and IP settings.

a) Disable DHCP. See [Network Configuration Menu](#) on page 57 for instructions.

b) Assign static IP values to the phone. See [Network Configuration Menu](#) on page 57 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 57 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. For more information, see [Configuring The IP Hosts File on a Windows 2000 Communications Manager Server](http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_tech_note09186a0080094976.shtml), available at this URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_tech_note09186a0080094976.shtml

**Step 4** From Cisco Unified Communications Manager, choose **System > Server** and verify that the server is referred to by its 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 37.

**Step 6** Power cycle the phone.

General Troubleshooting Information

This section provides troubleshooting information for some common issues that might occur on the Cisco Unified IP Phone.

The following table provides general troubleshooting information for the Cisco Unified IP Phone.

<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 (daisy chaining by using the PC port), the phones will not work.</td>
</tr>
<tr>
<td>Prolonged broadcast storms cause IP phones to re-register.</td>
<td>Prolonged broadcast storms (lasting several minutes) on the voice VLAN cause the IP phones to re-register with another Cisco Unified Communications Manager server.</td>
</tr>
<tr>
<td>Summary</td>
<td>Explanation</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</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’s network connection and plug the cable into a desktop computer. <strong>Caution</strong> The network card in the computer 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 there is no longer a phone 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 55 for details.</td>
</tr>
<tr>
<td>Phone resetting.</td>
<td>The phone resets when it loses contact with the Cisco Unified Communications Manager software. This lost connection can be due to any network connectivity disruption, including cable breaks, switch outages, and switch reboots.</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 or 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, reenable 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. See Network Configuration Menu, on page 57. (applies to Cisco Unified IP Phone 7911G only)                                                                                      |
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 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.

---

**Cisco Unified IP Phone Reset or Restore**

There are two methods 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>
<thead>
<tr>
<th>Operation</th>
<th>Action</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reset phone</td>
<td>From any screen (but not when the phone is idle), press <strong>##</strong>.</td>
<td>Resets any user and network configuration changes that you have made but that the phone has not written to its flash memory to previously saved settings, then restarts the phone.</td>
</tr>
</tbody>
</table>
Perform 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
- 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. The phone recovers by loading the term11.default.loads file.

Note

This phone must be on a DHCP-enabled network before you can perform these steps.

To perform a factory reset of a phone, perform these steps:

Procedure

Step 1  Plug in the power adapter to wake up the phone while sleeping. The phone begins its power-up cycle.

Step 2  While the phone is powering up, and before the Applications Menu button flashes on and off, press and hold #. Continue to hold # until the message LED on the handset flashes on and off in sequence in red.

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 will not take place.
After you press these keys, the message LED on the handset flashes faster in red, and the phone goes through the factory reset process.
Do not power down the phone until it completes the factory reset process, and the main screen appears.

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 includes these 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 the following statistical metrics that are based on concealment events. The Digital Signal Processor (DSP) plays concealment frames to mask frame loss in the voice packet stream.

- Concealment Ratio metrics: Shows the ratio of concealment frames over total speech frames. The phone calculates an interval conceal ratio every 3 seconds.
- Concealed Second metrics: Shows 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: Uses 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.

The phone uses the Cisco proprietary algorithm, Cisco Voice Transmission Quality (CVTQ) index, to produce MOS LQK scores. 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 or remotely by using Streaming Statistics.

### 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:

- G.711 codec gives 4.5 score
- G.729A/ AB gives 3.8 score
- G.728/iLBC gives 3.9 score

- CVTQ does not support wideband (7 kHz) speech codecs, because 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 50: 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>significantly increase significantly</td>
<td></td>
</tr>
<tr>
<td>Conceal Ratio is near or at zero,</td>
<td>Noise or distortion in the audio channel such as echo or audio levels.</td>
</tr>
<tr>
<td>but 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

- Internal Support Web Site Overview, page 203
- Cisco Unified IP Phone User Support, page 203
- User Options Web Pages Access, page 204
- Cisco Unified IP Phone Manuals, page 204
- Cisco Unified IP Phone 7900 Series eLearning Tutorials for SCCP Phones, page 204
- Phone Features User Subscription and Setup, page 205
- User Voice Messaging System Access, page 205
- User Personal Directory Entries Setup, page 206

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 end users. Cisco recommends that you create a web page on your internal support site that provides end users with important information about their Cisco Unified IP Phones.

This chapter describes information that you should make available on your support 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

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.

There are several Cisco Unified IP Phone models 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 users on your website.

For a list of available documentation, go to the Cisco Unified IP Phone website at this URL:


For the Cisco Unified Communications Manager documents, 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.
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 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/CCMUser/, where server_name is the host on which the web server is installed.
- A user ID and default password 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 124).
- 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 using the web page.

You can also refer users to Customizing Your Cisco Unified IP Phone on the Web, which is available at this URL:


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 205 for details.
- Cisco Unified IP Phone Address Book Synchronizer: Make sure to provide users with the installer for this application.
  - See Obtain Cisco Unified IP Phone Address Book Synchronizer, on page 206 to obtain the synchronizer.
  - See Cisco Unified IP Phone Address Book Synchronizer Deployment, on page 206 for instructions to send to your users.

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</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>To obtain the installer, choose Application &gt; Plugins from Cisco Unified Communications Manager Administration.</td>
</tr>
<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 206 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.
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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Get the Cisco Unified IP Phone Address Book Synchronizer installer file from your system administrator.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Double-click the TabSyncInstall.exe file that your administrator provided. The publisher dialog box displays.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Select <strong>Run</strong>. The Welcome to the InstallShield Wizard for Cisco Unified CallManager Personal Address Book Synchronizer window displays.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Select <strong>Next</strong>. The License Agreement window displays.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Read the license agreement information, and select the <strong>I Accept</strong>. Select <strong>Next</strong>. The Destination Location window displays.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Choose the directory in which you want to install the application and select <strong>Next</strong>. The Ready to Install window displays.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Select <strong>Install</strong>. The installation wizard installs the application to your computer. When the installation is complete, the InstallShield Wizard Complete window displays.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Select <strong>Finish</strong>.</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>To complete the process, follow the steps in <strong>Set Up Synchronizer</strong>, on page 207.</td>
</tr>
</tbody>
</table>

**Set Up Synchronizer**

To configure the Cisco Unified IP Phone Address Book Synchronizer, perform these steps:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Open the Cisco Unified IP Phone Address Book Synchronizer. If you accepted the default installation directory, you can open the application by choosing <strong>Start &gt; All Programs &gt; Cisco Systems &gt; TabSync</strong>.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>To configure user information, select <strong>User</strong>.</td>
</tr>
</tbody>
</table>
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.
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.

In most cases, the Cisco Unified IP Phone 7906G and 7911G support similar features whether on SCCP or SIP. 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, refer to the Cisco Unified IP Phone 7906G and 7911G User Guide for Cisco Unified Communications Manager (SCCP and SIP), which is available at this URL:


The specific sections that describe the features in the phone user guide are referenced in the following table.

### Table 51: Cisco IP Phone 7906G and 7911G 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>Calling features</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Abbreviated Dialing</td>
<td>Supported</td>
<td>Supported</td>
<td>Basic Call Handling—Placing a Call: Additional Options</td>
</tr>
<tr>
<td>Agent Greeting</td>
<td>Supported</td>
<td>Supported</td>
<td>Basic Call Handling—Answering a Call</td>
</tr>
<tr>
<td>Anonymous Call Block</td>
<td>Not Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Audible Message Waiting Indicator</td>
<td>Supported</td>
<td>Supported</td>
<td>Accessing Voice Messages</td>
</tr>
<tr>
<td>AutoAnswer</td>
<td>Supported</td>
<td>Supported</td>
<td>Using a Handset, Headset, and Speakerphone—Using Auto Answer</td>
</tr>
<tr>
<td>Auto Dial</td>
<td>Supported</td>
<td>Supported</td>
<td>Basic Call Handling—Placing a Call: Basic Options</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>Barge (and eBarge)</td>
<td>Supported</td>
<td>Supported</td>
<td>Advanced Call Handling—Using a Shared Line</td>
</tr>
<tr>
<td>Block External to External Transfers</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Call Back</td>
<td>Supported</td>
<td>Supported</td>
<td>Basic Call Handling—Placing a Call: Additional 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>Basic Call Handling—Forwarding Calls to Another Number</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>Basic Call Handling—Forwarding Calls to Another Number</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>Basic Call Handling—Forwarding Calls to Another Number</td>
</tr>
<tr>
<td>Call Park</td>
<td>Supported</td>
<td>Supported</td>
<td>Advanced Call Handling—Storing and Receiving Parked Calls</td>
</tr>
<tr>
<td>Call Pickup Group Call Pickup</td>
<td>Supported</td>
<td>Supported</td>
<td>Advanced Call Handling—Picking Up a Redirected Call on Your Phone</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>Basic Call Handling—Answering a Call</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>Caller ID</td>
<td>Supported</td>
<td>Supported</td>
<td>An Overview of Your Phone—Understanding Touch Screen Features or An Overview of Your Phone—Understanding Phone Screen Features</td>
</tr>
<tr>
<td>Caller ID Blocking</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Cisco 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>Client Matter Codes (CMC)</td>
<td>Supported</td>
<td>Not supported</td>
<td>Basic Call Handling—Placing a Call: Additional Options</td>
</tr>
<tr>
<td>Conference</td>
<td>Supported</td>
<td>Supported</td>
<td>Basic Call Handling—Making Conference Calls</td>
</tr>
<tr>
<td>Computer Telephony Integration (CTI) Applications</td>
<td>Supported</td>
<td>Some support (such as Call Park, WMI)</td>
<td>Users do not interact with this feature directly. It is configured on Cisco Unified Communications Manager</td>
</tr>
<tr>
<td>Device Invoked Recording</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Do Not Disturb (DND)</td>
<td>Supported</td>
<td>Supported</td>
<td>Basic Call Handling—Using Do Not Disturb</td>
</tr>
<tr>
<td>Directed Call Park</td>
<td>Supported</td>
<td>Supported</td>
<td>Advanced Call Handling—Storing and Receiving Parked Calls</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>Using Phone Settings—Customizing Rings and Message Indicators</td>
</tr>
<tr>
<td>Extension Mobility</td>
<td>Supported</td>
<td>Supported</td>
<td>Advanced Call Handling—Using Cisco Extension Mobility</td>
</tr>
<tr>
<td>Extension Mobility Change PIN</td>
<td>Supported</td>
<td>Supported</td>
<td>Advanced Call Handling—Using Cisco Extension Mobility</td>
</tr>
<tr>
<td>Extension Mobility Cross Cluster</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>External Call Control</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>Fast Dial Service</td>
<td>Supported</td>
<td>Supported</td>
<td>Advanced Call Handling—Speed Dialing</td>
</tr>
<tr>
<td>Forced Authorization Codes (FAC)</td>
<td>Supported</td>
<td>Not supported</td>
<td>Basic Call Handling—Placing a Call: Additional Options</td>
</tr>
<tr>
<td>Headset Sidetone Control</td>
<td>Not supported</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td>Help System</td>
<td>Supported</td>
<td>Supported</td>
<td>An Overview of Your Phone—Understanding Feature Buttons and Menus</td>
</tr>
<tr>
<td>Hold/Resume</td>
<td>Supported</td>
<td>Supported</td>
<td>Basic Call Handling—Using Hold and Resume</td>
</tr>
<tr>
<td>Hold Reversion</td>
<td>Supported</td>
<td>Supported</td>
<td>Basic Call Handling—Using Hold and Resume</td>
</tr>
<tr>
<td>Hold Status</td>
<td>Supported</td>
<td>Supported</td>
<td>Using Hold and Resume</td>
</tr>
<tr>
<td>Hunt Group</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Immediate Divert</td>
<td>Supported</td>
<td>Supported</td>
<td>Basic Call Handling—Answering a Call</td>
</tr>
<tr>
<td>Immediate Divert—Enhanced</td>
<td>Supported</td>
<td>Supported</td>
<td>Basic Call Handling—Sending a Call to a Voice Messaging System</td>
</tr>
<tr>
<td>Intelligent Session Control</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Intercom</td>
<td>Supported</td>
<td>Supported</td>
<td>Basic Call Handling—Placing or Receiving Intercom Calls</td>
</tr>
<tr>
<td>Inter-Cluster Trust (Bulk Certificate Replication)</td>
<td>Supported</td>
<td>Supported</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>Not supported</td>
<td>Basic Call Handling—Making Conference Calls</td>
</tr>
<tr>
<td>Join Across Lines</td>
<td>Supported</td>
<td>Not supported</td>
<td>Basic Call Handling—Making Conference Calls</td>
</tr>
<tr>
<td>Log Out of Hunt Groups</td>
<td>Supported</td>
<td>Supported</td>
<td>Advanced Call Handling—Logging Out of Hunt Groups</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>Malicious Call ID</td>
<td>Supported</td>
<td>Not supported</td>
<td>Advanced Call Handling—Tracing Suspicious Calls</td>
</tr>
<tr>
<td>Meet Me Conference</td>
<td>Supported</td>
<td>Supported</td>
<td>Basic Call Handling—Making Conference Calls</td>
</tr>
<tr>
<td>Message Waiting Indicator</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Missed call logging</td>
<td>Supported</td>
<td>Supported</td>
<td>Using Call Logs and Directories</td>
</tr>
<tr>
<td>Mobile Connect</td>
<td>Supported</td>
<td>Supported</td>
<td></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>Advanced Call Handling—Prioritizing Critical Calls</td>
</tr>
<tr>
<td>Multiple Calls per Line Appearance</td>
<td>200</td>
<td>50</td>
<td>An Overview of Your Phone—Understanding Lines vs. Calls</td>
</tr>
<tr>
<td>Mute</td>
<td>Supported</td>
<td>Supported</td>
<td>Basic Call Handling—Muting and Unmuting a Call</td>
</tr>
<tr>
<td>On-hook Dialing/Pre-Dial</td>
<td>Supported</td>
<td>Supported</td>
<td>Basic Call Handling—Placing a Call: Basic Options</td>
</tr>
<tr>
<td>Onhook Call Transfer</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Other Group Pickup</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Phone secure web access</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Plus Dialing</td>
<td>Supported</td>
<td>Supported</td>
<td>Using Call Logs</td>
</tr>
<tr>
<td>Presence-Enabled Directories</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Private Line Automated Ringdown (PLAR)</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Privacy</td>
<td>Supported</td>
<td>Supported</td>
<td>Advanced Call Handling—Using a Shared Line</td>
</tr>
<tr>
<td>Programmable Line Keys</td>
<td>Supported</td>
<td>Not supported</td>
<td>Feature descriptions throughout Cisco Unified IP Phone 7906G and 7911G User Guide for Cisco Unified Communications Manager</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>Quality Reporting Tool (QRT)</td>
<td>Supported</td>
<td>Supported</td>
<td>Troubleshooting—Using the Quality Reporting Tool</td>
</tr>
<tr>
<td>Redial</td>
<td>Supported</td>
<td>Supported</td>
<td>Basic Call Handling—Placing a Call: Basic Options</td>
</tr>
<tr>
<td>Ring Setting</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Ringer Volume Control</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Secure and Nonsecure Indication Tone</td>
<td>Supported</td>
<td>Supported</td>
<td>Advanced Call Handling—Making and Receiving Secure Calls</td>
</tr>
<tr>
<td>Secure Conference</td>
<td>Supported</td>
<td>Supported</td>
<td>Basic Call Handling—Making 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>Basic Call Handling—Switching an In-Progress Call to Another Phone</td>
</tr>
<tr>
<td>Shared Line</td>
<td>Supported</td>
<td>Supported</td>
<td>Advanced Call Handling—Using a Shared Line</td>
</tr>
<tr>
<td>Silent Monitoring</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Single Button Barge</td>
<td>Supported</td>
<td>Not supported</td>
<td>Advanced Call-Handling—Using Barge to Add Yourself to a Shared-Line Call</td>
</tr>
<tr>
<td>Speed Dialing</td>
<td>Supported</td>
<td>Supported</td>
<td>Advanced Call Handling—Speed Dialing</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>Time Zone Update</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>Basic Call Handling—Transferring Calls</td>
</tr>
<tr>
<td>URL Dialing</td>
<td>Not supported</td>
<td>Supported</td>
<td>Using Call Logs and Directories—Using Call Logs</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>Video Support</td>
<td>Supported</td>
<td>Not supported</td>
<td>Understanding Additional Configuration 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>Accessing Voice Messages section of <em>Cisco Unified IP Phone 7906G and 7911G User Guide for Cisco Unified Communications Manager</em></td>
</tr>
<tr>
<td>WebDialer</td>
<td>Supported</td>
<td>Supported</td>
<td>Customizing Your Phone on the Web—Configuring Features and Services on the Web</td>
</tr>
</tbody>
</table>

**Settings**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Protocol: SCCP</th>
<th>Protocol: SIP</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic Port Synchronization</td>
<td>Supported</td>
<td>Supported</td>
<td>Cisco Unified IP Phone 7906G does not support Automatic Port Synchronization.</td>
</tr>
<tr>
<td>Call Statistics</td>
<td>Supported</td>
<td>Supported</td>
<td>Troubleshooting Your Phone—Viewing Phone Administrative Data</td>
</tr>
<tr>
<td>Power Save Plus (EnergyWise)</td>
<td>Supported</td>
<td>Not supported</td>
<td>An Overview of the Cisco Unified IP Phone—Reducing Power Consumption on the Phone</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>Configuring Features, Templates, Services, and Users—Telephony Features Available for the Cisco Unified IP Phone</td>
</tr>
<tr>
<td>UCR 2008</td>
<td>Supported</td>
<td>Not supported</td>
<td>Configuring Features, Templates, Services, and Users—Telephony Features Available for the Cisco Unified IP Phone</td>
</tr>
<tr>
<td>Voice Quality Metrics</td>
<td>Supported</td>
<td>Supported</td>
<td>Troubleshooting Your Phone—Viewing Phone Administrative Data</td>
</tr>
</tbody>
</table>

**Services**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Protocol: SCCP</th>
<th>Protocol: SIP</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SDK Compliance</td>
<td>Supported</td>
<td>Supported</td>
<td><em>Cisco Unified IP Phone Service Application Development Notes for Release 4.1(3) or later</em></td>
</tr>
</tbody>
</table>

**Directories**
<table>
<thead>
<tr>
<th>Features</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>Using Call Logs and Directories—Directory Dialing</td>
</tr>
<tr>
<td>Corporate Directories</td>
<td>Supported</td>
<td>Supported</td>
<td>Using Call Logs and Directories—Directory Dialing</td>
</tr>
<tr>
<td>Personal Directory Enhancements</td>
<td>Supported</td>
<td>Supported</td>
<td>Using Call Logs and Directories—Directory Dialing</td>
</tr>
</tbody>
</table>

**Supplemental features and applications**

<table>
<thead>
<tr>
<th>Feature</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>Not supported</td>
<td>Cisco Unified Communications Manager Features and Services Guide</td>
</tr>
<tr>
<td>Cisco Unified Department Attendant Console</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco Unified Enterprise Attendant Console</td>
<td></td>
<td></td>
<td></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>

<table>
<thead>
<tr>
<th>Feature</th>
<th>Protocol: SCCP</th>
<th>Protocol: SIP</th>
<th>For more information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified IP Phone Expansion Module 7914</td>
<td>Not supported</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td>Cisco Unified IP Phone Expansion Module 7915</td>
<td>Not supported</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td>Cisco Unified IP Phone Expansion Module 7916</td>
<td>Not supported</td>
<td>Not supported</td>
<td></td>
</tr>
</tbody>
</table>
International User Support

- International User Support Overview, page 217
- Unified Communications Manager Endpoints Locale Installer, page 217
- Language Limitation, page 218
- International Call Logging Support, page 218

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, see the following sections to ensure that the phones are set up properly for your users.

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 219
- Cable Specifications, page 220
- Network and Access Port Pinouts, page 220
- Phone Behavior During Times of Network Congestion, page 222

Physical and Operating Environment Specifications

The following table shows the physical and operating environment specifications for the Cisco Unified IP Phones.

Table 52: 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>6.5 in. (20.3 cm)</td>
</tr>
<tr>
<td>Width</td>
<td>7 in. (17.67 cm)</td>
</tr>
<tr>
<td>Depth</td>
<td>6 in. (15.2 cm)</td>
</tr>
<tr>
<td>Weight</td>
<td>1.9 lb (0.9 kg)</td>
</tr>
</tbody>
</table>
### Cable Specifications

- RJ-9 jack (4-conductor) for handset and headset connection.
- RJ-45 jack for the LAN 10/100BaseT connection (labeled 10/100 SW).
- RJ-45 jack for the access port 10/100BaseT connection (labeled 10/100 PC).
- 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>
</tbody>
</table>

---

**Note**

Cables have 4 pairs of wires for a total of 8 conductors.

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).

---

**Table 53: Network Port Connector Pinouts**
Computer Port Connector

The following table describes the computer port connector pinouts.

**Table 54: 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 223
- Example User Information, page 223
- Cisco Unified Communications Manager User Addition, page 224
- Phone Setup, page 225
- Perform Final End User Setup, page 228

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

For more information and limitations on configuring LDAP system, see the Cisco Unified Communications Manager Administration Guide, "LDAP System Configuration", "LDAP Directory Configuration", and the "LDAP Authentication Configuration" chapters and Cisco Unified Communications Manager System Guide, "Understanding the Directory" chapter.

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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Log onto Cisco Unified Communications Manager Administration.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Choose System &gt; LDAP &gt; LDAP Directory.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Use the Find button to locate your LDAP directory.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click on the LDAP directory name.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Perform Full Sync Now.</td>
</tr>
<tr>
<td>Note</td>
<td>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.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Proceed to Phone Setup, on page 225.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose User Management &gt; End User, then click Add New. The End User Configuration window appears.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the User Information pane of this window, enter the following:</td>
</tr>
</tbody>
</table>
Basic Phone Administration Steps

Note

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>From Cisco Unified Communications Manager administration, choose Device &gt; Phone.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click Add New.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select the user phone model from the Phone Type drop-down list, then click Next.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Select the device protocol (SCCP or SIP) from the drop-down list, then click Next. The Phone Configuration window appears.</td>
</tr>
</tbody>
</table>

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, sofkey 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.

   - **Sofkey Template**: Choose the appropriate sofkey template. The sofkey template determines the configuration of the sofkeys on Cisco Unified IP Phones. Leave this field blank if the common device configuration contains the assigned sofkey template.

**Note**  
Sofkey templates are defined on the Sofkey Template Configuration window of Cisco Unified Communications Manager Administration (Device > Device Settings > Sofkey Template). You can use the search fields in conjunction with the Find button to find all configured sofkey 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 228.

---

**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**.
Basic Phone Administration Steps

Perform Final End User Setup
INDEX

.cnf.xml configuration file 31
"more" Softkey Timer 76

10/100 PC port 41
   See also access port
10/100 SW port 41
   See also network port
10/100/1000 PC port 41
802.1X 3, 18
   authentication 18
   authentication server 18
   authenticator 18
   description 3
   network components 18
   supplicant 18
802.1x authentication and status 94
802.1X Authentication menu 89, 94
   about 89
   options 94
   Device Authentication 94
802.1X Authentication Status menu 89, 94
   about 89
   states 94

A
abbreviated dialing 98, 209
AC adapter 44
   connecting 44
access 51, 54
   to phone settings 51, 54
access port 41, 44, 57, 79, 80
   10/100 PC 41
   10/100/1000 PC 41
   configuring 57
   connecting 44
   disabled 80
   forwarding packets to 79
   access to phone settings 53

Access web page 164, 171
adding 33, 35, 124
   Cisco Unified IP Phones manually 35
   Cisco Unified IP Phones using auto-registration 33
   Cisco Unified IP Phones using BAT 35
   users to Cisco Unified Communications Manager 124
Address Book Synchronization Tool (TABSynch) 206, 207
   configuring 207
   installing 206, 207
   obtaining 206
Admin. VLAN ID 57
AdvanceAdhocConference service parameter 98
agent greeting 209
Alternate TFTP 57
Anonymous Call Block 209
any call pickup 98
Applications Menu button 2
audible message waiting indicator 209
Audible message waiting indicator 98
authenticated call 14
authentication 10, 51
authentication server 18
   in 802.1X 18
Authentication URL 74
authenticator 18
   in 802.1X 18
auto answer 98, 209
Auto Call Select 76
   auto dial 209
   auto-registration 33
   using 33
AutoAttendant 209
automatic port synchronization 209
auxiliary VLAN 28

B
background image 138, 139
   configuring 139
   creating 138
   custom 138
background image (continued)

Cisco Catalyst Switch 18
Cisco Discovery Protocol, See CDP
Cisco Extension Mobility 98
Cisco Extension Mobility Cross Cluster (EMCC) 98
Cisco Peer to Peer Distribution Protocol (CPPDP) 3
Cisco Secure Access Control Server (ACS) 18
Cisco Unified Communications Manager 28, 33, 40, 182, 209
adding phone to database of 33
AutoAttendant 209
interactions with 28
required for Cisco Unified IP Phones 40
verifying settings 182
Cisco Unified Communications Manager Administration 98
adding telephony features using 98
Cisco Unified Communications Manager Assistant 209
Cisco Unified IP Phone 2, 3, 21, 29, 33, 35, 44, 49, 119, 120, 124, 163,
201, 219
adding manually to Cisco Unified Communications
Manager 35
adding to Cisco Unified Communications Manager 33
cleaning 201
configuration requirements 21
configuring user services 124
features 2
figure 2
illustration 2
installation overview 21
installation procedure 44
installation requirements 21
modifying phone button templates 120
mounting to wall 49
power sources 29
registering 33
registering with Cisco Unified Communications Manager 33,
35
supported networking protocols 3
technical specifications 219
using LDAP directories 119
web page 163
Cisco Unified IP Phone Expansion Module 7914 209
7915, and 7916 209
Cisco VT Advantage 209
cleaning the Cisco Unified IP Phone 201
Clear softkey 145, 152
client matter codes 98, 209
computer telephony integration (CTI) applications 209
conference 15, 98, 209
secure 15
conference joining 98
conferencing 209
secure 209
Configuration 127
Power Save 127
configuration file 31, 194
.cnf.xml 31
creating 194
overview 31
XmlDefault.cnf.xml 31
Configuration Parameters 118
configuring 21, 50, 55, 119, 123, 124, 127
from a Cisco Unified IP Phone 55
LDAP directories 119
overview 21
personal directories 120
phone button templates 120
Power Save 127
softkey templates 123
startup network settings 50
user features 124
connecting 44
handset 44
to a computer 44
to AC adapter 44
to the network 44
Console Logs web page 164
Core Dumps web page 164
corporate directories 209
CTL file 32, 197
deleting from phone 197
requesting 32
CTL File screen 90
custom phone rings 136, 137, 139
about 136
creating 136, 137, 139
PCM file requirements 137

daisy chaining 195
data VLAN 28
Debug Display web page 164, 174
Default Router 1-5 57
device authentication 12
Device Configuration menu 94
Device Configuration menu 53, 54, 55, 69
displaying 54
editing values 55
overview 53
sub-menus 69
Device Information web page 164, 166
device invoked recording 98
DHCP 3, 57, 185, 191
description 3
IP address 191
troubleshooting 185
DHCP Address Released 57
DHCP Server 57
DHCPv6 57
DHCPv6 Address Released 57
direct transfer 98
directed call park 98, 209
directed call pickup 98
Directories URL 74
directory 209
corporate 209
personal 209
directory numbers 35
assigning manually 35
disable 76
Disabling Enbloc Dialing 209
distinctive ring 209
DND 98
DNS server 182, 186
troubleshooting 186
verifying settings 182
DNS Server 1-5 57
do not disturb 98, 209
Domain Name 57
Domain Name System (DNS) 57
Domain Name System (DNS) server 57
DSCP For Call Control 82
DSCP For Configuration 82
DSCP For Services 82
Dynamic Host Configuration Protocol, See DHCP

E

EAP-MD5 94
description 94
Device ID 94
Realm 94
Shared Secret 94
editing 55
configuration values 55
Enbloc Dialing 76
encryption 10, 12
about 10
media 12
EnergyWise 21, 127
description 21
troubleshooting 185
enterprise parameters 126
call forward 126
call forward options 126
user options web page defaults 126
Erase softkey 197
error messages 180
used for troubleshooting 180
Ethernet Configuration menu 79
about 79
Span to PC Port option 79
Ethernet Information web page 164, 171
extension mobility 209

F
fast dial 209
fast dial service 98
features 9
configuring on phone, overview 9
configuring with Cisco Unified Communications Manager, overview 9
informing users about 9
figure 2
Cisco Unified IP Phone features 2
file authentication 12
file format 136, 138
List.xml 138
RingList.xml 136
firmware 156
verifying version 156
Firmware Versions screen 156
footstand 46
installing 46
forced authorization codes 98, 209

G
G.722 codec 78
GARP Enabled 80
group call pickup 98, 209
Group Listen 76
Group Listen mode 42

H
handset 2, 44
connecting 44
light strip 2
headset 43, 44
audio quality 44
quality 44
using 43
headset port 44
help system 209
hold 98, 209
hold status 98
ihold 209
hold button illustration 2
hold reversion 98, 209
hold status 98
Host Name 57
HTTP 166
HTTP Configuration menu 74
about 74
Authentication URL 74
Directories URL 74
Idle URL 74
Idle URL Time 74
Information URL 74
Messages URL 74
Proxy Server URL 74
Services URL 74
HTTPS 3, 166
description 3
hunt group 98
log out of hunt groups 98
hunt group display 98, 209
hunt groups 209
log out 209

I
icon 14
lock 14
padlock 14
shield 14
idle display 74
timeout 74
XML service 74
Idle URL 74
Idle URL Time 74
ihold 209
image authentication 12
immediate divert 98, 209
Immediate Divert enhanced feature 98
Information URL 74
installing 21, 33, 39, 40, 44
Cisco Unified Communications Manager configuration 40
network requirements 39
preparing 33
procedure 44
requirements, overview 21
Intelligent Session Control 98, 209
intercom 209
interference 1
cell phone 1
Internet Protocol (IP) 3
IP address 182
troubleshooting 182
IP Address 57
IPv4 Configuration 57
IPv6 Address 57
IPv6 Alternate TFTP 57
IPv6 Configuration 57
IPv6 Default Router 1-2 57
IPv6 DNS Server 1-2 57
IPv6 Load server 82
IPv6 Log server 82
IPv6 on the Cisco Unified IP Phone 8
IPv6 Prefix Length 57

logging 98, 209
missed call 98, 209
LSC (locally significant certificate) 144

MAC address 57
malicious call ID 209
malicious call identification (MCID) 98
manufacturing installed certificate (MIC) 12
Media Configuration menu 78
about 78
Speaker Enabled option 78
media encryption 12
Meet Me conference 98
meet-me conference 209
message waiting 98
Message Waiting Indicator 209
messages (status) 145
Messages URL 74
metrics 175
voice quality 175
MIC 12, 144
missed call logging 98, 209
MLPP 209
mobile connect 98
Mobile Connect 209
mobile voice access 98
Mobile Voice Access 209
Model Information screen 143
Monitor mode 42
multilevel precedence and preemption 209
multilevel precedence and preemption (MLPP) 98
multiple calls per line 209
Music on Hold 98
mute 209

native VLAN 28
navigation button illustration 2
Network Configuration Area items 167
LLDP on PC port 167
LLDP-MED on SW port 167
Network Configuration menu 53, 54, 55, 57, 82, 160, 167
about 57
Admin. VLAN ID 57
CDP on PC port 82
CDP on switch port 82
displaying 54
Domain Name 57
Network Configuration menu (continued)
editing values 55, 160
Host Name 57
IPv4 57
  Alternate TFTP 57
  BOOTP Server 57
  Default Router 1-5 57
  DHCP 57
  DHCP Address Released 57
  DHCP Server 57
  DNS Server 1-5 57
  IP Address 57
  Subnet Mask 57
  TFTP Server 1 57
  TFTP Server 2 57
IPv6 57
  DHCPv6 57
  DHCPv6 Address Released 57
  IPv6 Address 57
  IPv6 Alternate TFTP 57
  IPv6 Default Router 1-6 57
  IPv6 DNS Server 1-2 57
  IPv6 Prefix Length 57
 LLDP Asset ID 82
 LLDP-MED ID 82
locking options 55
options 57, 82, 167
  CDP on PC port 167
  LLDP on PC port 82
  LLDP power priority 82
  MAC Address 57
  Operational VLAN ID 57
  PC Port Configuration 57
  PC VLAN 57
  SW Port Configuration 57
overview 53
unlocking options 55
Network Configuration web page 164, 167
  network connectivity 181
    verifying 181
  Network Locale 75
    description 75
    version 75
  network outages 184
    identifying 184
  network port 41, 44, 57
    10/100 SW 41
    configuring 57
    connecting to 44
  network requirements 39
    for installing 39
  network settings 50
    startup configuration 50
  network statistics 152, 171
Network Statistics screen 152
Network web page 164, 171
  networking protocol 3
    802.1X 3
    BootP 3
    CDP 3
    CPPDP 3
    DHCP 3
    IP 3
    LLDP 3
    LLDP-MED 3
    RTCP 3
    RTP 3
    SCCP 3
    SIP 3
    SRTP 3
    TCP 3
    TFTP 3
    TLS 3
    UDP 3
  networking protocols 3
    supported 3

O
  on-hook call transfer 98
  on-hook dialing/pre-dial 209
  Onhook Call Transfer 209
  Operational VLAN ID 57
    options 126
      enterprise parameters 126
      user options web page defaults 126
  other group pickup 98
  Other Group Pickup 209

P
  padlock icon 14, 55, 160
  PC 41
    connecting to the phone 41
      PC Port Configuration 57
      PC Port Disabled 80
      PC VLAN 57
    PCM file requirements 137
      for custom ring types 137
    Peer firmware sharing 82
    personal directories 120
    personal directory 209
    phone button templates 120
      modifying 120
    phone configuration checklist (table) 22
phone settings access 53
physical connection 184
verifying 184
plugging in Cisco Unified IP Phone 44
plus dialing 209, 218
PNG file 138, 139
power 21, 29, 30, 127
   EnergyWise 21
   EnergyWise configuration 127
   EnergyWise description 21
   outage 30
   providing to the Cisco Unified IP Phone 29
Power over Ethernet (PoE) 29
power source 29, 186
   causing phone to reset 186
   description 29
   external power 29
   PoE 29
   power injector 29
Presence-Enabled Directories 209
privacy 98, 209
private line automated ringdown 98
Private Line Automated Ringdown (PLAR) 209
programmable line keys 209
protected call 16
   description 16
protected calling 98
   description 98
Protected Calls 16
Proxy Server URL 74

Q
QoS Configuration menu 82
   about 82
   options 82
      DSCP For Call Control 82
      DSCP For Configuration 82
      DSCP For Services 82
QRT 209
QRT softkey 98, 199
quality reporting tool 209
Quality Reporting Tool (QRT) 98, 199

R
Real-Time Control Protocol, See RTCP
Real-Time Transport Protocol, See RTP
redial 98, 209
remote port configuration 209
reset 198
   factory 198
resetting 184, 185, 197
   basic 197
   continuously 184
   intentionally 185
   methods 197
resume 209
ring setting 98
Ring Setting 209
ringer 2
   indicator for 2
RingList.xml file format 136

S
SCCP 3
   description 3
SDK compliance 209
secure and nonsecure indication tone 98, 209
secure conference 15, 16, 98
   description 15, 98
   establishing 15
   identifying 15
   restrictions 16
secure conferencing 209
Secure Real-Time Transport Protocol, See RTP
security 12, 51
   configuring on phone 51
   device authentication 12
   file authentication 12
   image authentication 12
   Locally Significant Certificate (LSC) 51
   media encryption 12
   signaling authentication 12
Security Configuration menu (on Device Configuration menu) 80
   about 80
   options 80
      GARP Enabled 80
      Logging Display 80
      PC Port Disabled 80
      Security Mode 80
      Voice VLAN Enabled 80
      Web Access Enabled 80
Security Configuration menu (on Settings menu) 53, 89
   about 89
   options 89
      802.1X Authentication 89
      802.1X Authentication Status 89
      IPv6 CAPF Server 89
      LSC 89
      MIC 89
Security Configuration menu (on Settings menu) *(continued)*

- Security Mode 89
- Trust List 89
- Web Access Enabled 89

overview 53

Security Mode 80

select 209

services 98, 124
- configuring for users 124
- description 98
- subscribing to 124

Services 209

Services URL 74

Services URL button 98

Services URL Button 209

session handoff 98

Session Handoff 209

Settings menu access 51, 54

shared line 98, 209

shield icon 14

signaling authentication 12

silent monitoring 98

Silent Monitoring 209

single button barge 209

SIP 3

- description 3

SIP Configuration menu 70

SIP General Configuration menu 70

softkey buttons 2

- description of 2

softkey templates 123

- configuring 123

Span to PC Port 79

speaker 41

- about 41

- disabling 41

Speaker Enabled 78

speed dial 98

speed dialing 98, 209

standard (ad hoc) conference 98

startup problems 179

startup process 32, 50

- accessing TFTP server 32

- configuring VLAN 32

- obtaining IP address 32

- obtaining power 32

- requesting CTL file 32

- understanding 32

- verifying 50

- statistics 152, 171, 175

- network 152, 171

- streaming 175

- Status menu 143, 145

  - about 143

  - options 145

  - 802.1X Authentication Status 145

- Status Messages screen 145

- Status Messages web page 164, 174

- Stream 0 web page 175

- Stream 1 web page 164, 175

- Stream 2 web page 164, 175

- Stream 3 web page 164, 175

- streaming statistics 175

- Subnet Mask 57

- supplicant 18

  - in 802.1X 18

- SW Port Configuration 57

T

- TABSynch 206, 207

  - configuring 207

  - installing 206, 207

  - obtaining 206

- TCP 3

  - technical specifications 219

    - for Cisco Unified IP Phone 219

  - telephony features 20, 82

    - barge 20

    - IPv6 Log server 82

    - Log server 82

    - Peer firmware sharing 82

- TFTP 3, 181

  - description 3

  - troubleshooting 181

- TFTP Server 1 57

- TFTP Server 2 57

- TFTP settings 57

  - IPv6 57

  - time 39

    - displayed on phone 39

  - time zone update 98

  - Time-of-day Routing 209

  - Time-of-Day Routing 98

- TLS 31

  - touchscreen, See LCD screen

  - Touchscreen Illumination Disabling 209

  - transfer 209

- Transmission Control Protocol, See TCP

- Transport Layer Security, See TLS

- Trivial File Transfer Protocol, See TFTP

  - troubleshooting 181, 182, 184, 185, 186

  - Cisco Unified Communications Manager settings 182

  - DHCP 185
troubleshooting (continued)
  DNS 186
  DNS settings 182
  IP addressing and routing 182
  network connectivity 181
  network outages 184
  phones resetting 185
  physical connection 184
  services on Cisco Unified Communications Manager 182
  TFTP settings 181
  VLAN configuration 185

Trust List menu 93

U

UCR 2008 20, 130, 183
  POST definition 20
  POST update error 183
  Security Error message 183
  setting up 130
  supporting 20

UDI 166

UI Configuration menu 76
  about 76
  options 76
    Auto Call Select 76
    Group Listen 76

Unified CM Configuration menu 69

URL dialing 209

User Datagram Protocol, See UDP

User Locale 75
  character set 75
  description 75
  version 75

User Options web page 125, 126, 204
  call forward settings 126
  giving users access to 125, 204

users 124, 203, 204, 205, 206
  accessing voice messaging system 205
  adding to Cisco Unified Communications Manager 124
  configuring personal directories 206
  documentation for 204
  providing required information to 203
  providing support to 203
  subscribing to services 205
  using phone templates to add phones 35

V

verifying 50, 156
  firmware version 156

verifying (continued)
  startup process 50
  video 98, 209
    mode 98
    support 98
  VLAN 28, 57, 185
    auxiliary, for voice traffic 28
    configuring 57
    configuring for voice networks 28
    native, for data traffic 28
    verifying 185
  voice mail 209
  voice messaging system 98, 205
    accessing 205
  voice quality metrics 175, 209
  voice VLAN 28
  Voice VLAN Enabled 80
  volume button illustration 2

W

wall mounting 49

Web Access Enabled 80

web page 163, 164, 165, 166, 167, 171, 174, 175
  about 163
  Access 164, 171
  accessing 164
  Console Logs 164
  Core Dumps 164
  Debug Display 164, 174
  Device Information 164, 166
  disabling access to 165
  Ethernet Information 164, 171
  Network 164, 171
  Network Configuration 167
  Network Configuration web page 164
  preventing access to 165
  Status Messages 164, 174
  Stream 0 175
  Stream 1 164, 175
  Stream 2 164, 175
  Stream 3 164, 175

WebDialer 209

wideband handset 76, 78
  option 76
  user controllable 76

X

XmlDefault.cnf.xml 31