



## **Cisco Unified IP Phone 7960G/7940G Administration Guide for Cisco Unified Communications Manager 7.0 (SCCP)**

### **Americas Headquarters**

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

Text Part Number: OL-15498-01

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: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

- Turn the television or radio antenna until the interference stops.
- Move the equipment to one side or the other of the television or radio.
- Move the equipment farther away from the television or radio.
- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

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

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

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

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

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0805R)

*Cisco Unified IP Phone 7960G/7940G Administration Guide for Cisco Unified Communications Manager 7.0 (SCCP)*  
Copyright © 2008 Cisco Systems, Inc. All rights reserved.



## CONTENTS

### **Preface**    **xiii**

- Overview    **xiii**
- Audience    **xiii**
- Organization    **xiii**
- Related Documentation    **xiv**
- Obtaining Documentation, Obtaining Support, and Security Guidelines    **xv**
  - Cisco Product Security Overview    **xv**
- Document Conventions    **xv**

---

### **CHAPTER 1**

### **An Overview of the Cisco Unified IP Phone**    **1-1**

- Understanding the Cisco Unified IP Phones 7960G and 7940G    **1-1**
- What Networking Protocols Are Used?    **1-4**
- What Features are Supported on the Cisco Unified IP Phones 7960G and 7940G?    **1-5**
  - Feature Overview    **1-6**
  - Configuring Telephony Features    **1-6**
  - Configuring Network Parameters Using the Cisco Unified IP Phone    **1-7**
  - Providing Users with Feature Information    **1-7**
- Understanding Security Features for Cisco Unified IP Phones    **1-7**
  - Overview of Supported Security Features    **1-9**
  - Understanding Security Profiles    **1-10**
  - Identifying Encrypted and Authenticated Phone Calls    **1-11**
  - Security Restrictions    **1-11**
  - CAPF Interaction when the Phone Resets    **1-12**
- Overview of Configuring and Installing Cisco Unified IP Phones    **1-12**
  - Configuring Cisco Unified IP Phones in Cisco Unified Communications Manager    **1-13**
    - Checklist for Configuring the Cisco Unified IP Phone 7960G and 7940G in Cisco Unified Communications Manager    **1-13**
  - Installing Cisco Unified IP Phones    **1-16**
    - Checklist for Installing the Cisco Unified IP Phone 7960G and 7940G    **1-16**

---

### **CHAPTER 2**

### **Preparing to Install the Cisco Unified IP Phone on Your Network**    **2-1**

- Understanding Interactions with Other Cisco Unified IP Communications Products    **2-2**
  - Understanding How the Cisco Unified IP Phone Interacts with Cisco Unified Communications Manager    **2-2**

- Understanding How the Cisco Unified IP Phone Interacts with the VLAN 2-3
- Providing Power to the Cisco Unified IP Phone 2-3
  - Power Guidelines 2-4
  - Power Outage 2-4
  - Obtaining Additional Information about Power 2-4
- Understanding Phone Configuration Files 2-5
- Understanding the Phone Startup Process 2-6
- Adding Phones to the Cisco Unified Communications Manager Database 2-7
  - Adding Phones with Auto-Registration 2-8
  - Adding Phones with Auto-Registration and TAPS 2-9
  - Adding Phones with Cisco Unified Communications Manager Administration 2-9
  - Adding Phones with BAT 2-10
- Using Cisco Unified IP Phones with Different Protocols 2-10
  - Converting a New Phone from SCCP to SIP 2-10
  - Converting an In-Use Phone from SCCP to SIP 2-11
  - Converting an In-Use Phone from SIP to SCCP 2-11
  - Deploying a Phone in an SCCP and SIP Environment 2-11
- Determining the MAC Address for a Cisco Unified IP Phone 2-12

**CHAPTER 3**

**Setting Up the Cisco Unified IP Phone 3-1**

- Before You Begin 3-1
  - Network Requirements 3-2
  - Cisco Unified Communications Manager Configuration 3-2
- Understanding the Cisco Unified IP Phone 7960G and 7940G Components 3-2
  - Network and Access Ports 3-3
  - Handset 3-3
  - Speakerphone 3-3
  - Headset 3-3
    - Audio Quality Subjective to the User 3-4
    - Connecting a Headset 3-4
    - Disabling a Headset 3-4
    - Using External Devices with Your Cisco Unified IP Phone 3-4
- Installing the Cisco Unified IP Phone 3-5
- Attaching the Cisco Unified IP Phone Expansion Module 7914 3-7
- Adjusting the Placement of the Cisco Unified IP Phone 3-8
  - Adjusting Cisco Unified IP Phone Footstand and Phone Height 3-8
  - Mounting the Phone to the Wall 3-8
- Verifying the Phone Startup Process 3-9

- Configuring Startup Network Settings 3-10
- Configuring Security on the Cisco Unified IP Phone 3-10

**CHAPTER 4****Configuring Network Settings on the Cisco Unified IP Phone 4-1**

- Displaying the Network Configuration Menu 4-1
- Unlocking and Locking Options 4-2
- Editing Values 4-3
- Overview of Network Configuration Options 4-3
- Network Configuration Menu 4-4
  - Cisco Unified Communications Manager Options 4-10

**CHAPTER 5****Configuring Features, Templates, Services, and Users 5-1**

- Telephony Features Available for the Cisco Unified IP Phone 5-2
- Creating Custom Phone Rings 5-9
- Configuring Corporate and Personal Directories 5-9
  - Configuring Corporate Directories 5-9
  - Configuring Personal Directory 5-9
- Modifying Phone Button Templates 5-10
- Configuring Softkey Templates 5-11
- Setting Up Services 5-11
- Adding Users to Cisco Unified Communications Manager 5-12
- Managing the User Options Web Pages 5-12
  - Giving Users Access to the User Options Web Pages 5-12
  - Specifying Options that Appear on the User Options Web Pages 5-12

**CHAPTER 6****Viewing Model Information, Status, Statistics, and Security Information on the Cisco Unified IP Phone 6-1**

- Model Information Screen 6-2
- Status Menu 6-2
  - Status Messages Screen 6-3
  - Network Statistics Screen 6-7
  - Firmware Versions Screen 6-8
  - Expansion Module Stats Screen 6-9
- Call Statistics Screen 6-10
- Security Configuration Menu 6-12
  - CTL File Menu 6-12
  - Trust List Menu 6-14

**CHAPTER 7**

**Monitoring the Cisco Unified IP Phone Remotely 7-1**

- Accessing the Web Page for a Phone 7-2
- Disabling and Enabling Web Page Access 7-3
- Device Information 7-3
- Network Configuration 7-4
- Network Statistics 7-7
  - Ethernet Statistics 7-7
  - Port 1 (Network), Port 2 (Access), and Port 3 (Phone) Statistics 7-8
- Device Logs 7-10
  - Stack Statistics 7-11
  - Status Messages 7-11
- Streaming Statistics 7-11

**CHAPTER 8**

**Troubleshooting and Maintenance 8-1**

- Resolving Startup Problems 8-1
  - Symptom: The Cisco Unified IP Phone Does Not Go Through its Normal Startup Process 8-2
  - Symptom: The Cisco Unified IP Phone Does Not Register with Cisco Unified Communications Manager 8-2
    - Identifying Error Messages 8-3
    - Registering the Phone with Cisco Unified Communications Manager 8-3
    - Checking Network Connectivity 8-3
    - Verifying TFTP Server Settings 8-3
    - Verifying IP Addressing and Routing 8-4
    - Verifying DNS Settings 8-4
    - Verifying Cisco Unified Communications Manager Settings 8-4
    - Cisco Unified Communications Manager and TFTP Services Are Not Running 8-4
    - Creating a New Configuration File 8-5
    - Symptom: Cisco Unified IP Phone Unable to Obtain IP Address 8-6
- Cisco Unified IP Phone Resets Unexpectedly 8-6
  - Verifying Physical Connection 8-6
  - Identifying Intermittent Network Outages 8-7
  - Verifying DHCP Settings 8-7
  - Checking Static IP Address Settings 8-7
  - Verifying Voice VLAN Configuration 8-7
  - Verifying that the Phones Have Not Been Intentionally Reset 8-8
  - Eliminating DNS or Other Connectivity Errors 8-8
- Troubleshooting Cisco Unified IP Phone Security 8-9
- General Troubleshooting Tips 8-10

General Troubleshooting Tips for the Cisco Unified IP Phone Expansion Module 7914	8-12
Resetting or Restoring the Cisco Unified IP Phone	8-13
Performing a Basic Reset	8-13
Performing a Factory Reset	8-14
Using the Quality Report Tool	8-15
Monitoring the Voice Quality of Calls	8-15
Where to Go for More Troubleshooting Information	8-17
Cleaning the Cisco Unified IP Phone	8-17

**APPENDIX A****Providing Information to Users Via a Website** A-1

How Users Obtain Support for the Cisco Unified IP Phone	A-1
Giving Users Access to the User Options Web Pages	A-1
How Users Get Copies of Cisco Unified IP Phone Manuals	A-2
Accessing Cisco 7900 Series Unified IP Phone eLearning Tutorials	A-2
How Users Subscribe to Services and Configure Phone Features	A-2
How Users Access a Voice Messaging System	A-3
How Users Configure Personal Directory Entries	A-3
Installing and Configuring the Cisco Unified IP Phone Address Book Synchronizer	A-4

**APPENDIX B****Feature Support by Protocol for Cisco Unified IP Phone 7960G and 7940G** B-1**APPENDIX C****Supporting International Users** C-1

Adding Language Overlays to Phone Buttons	C-1
Installing the Cisco Unified Communications Manager Locale Installer	C-1

**APPENDIX E****Technical Specifications** E-1

Physical and Operating Environment Specifications	E-1
Cable Specifications	E-2
Network and Access Port Pinouts	E-2

**APPENDIX F****Basic Phone Administration Steps** F-1

Example User Information for these Procedures	F-1
Adding a User to Cisco Unified Communications Manager	F-2
Adding a User From an External LDAP Directory	F-2
Adding a User Directly to Cisco Unified Communications Manager	F-2
Configuring the Phone	F-3

**Performing Final End User Configuration Steps** F-8







# Preface

---

## Overview

*Cisco Unified IP Phone 7960G/7940G Administration Guide for Cisco Unified Communications Manager 7.0 (SCCP)* provides the information you need to understand, install, configure, and manage the Cisco Unified IP Phones 7960G and 7940G on your network.

## Audience

Network engineers, system administrators, or telecom engineers should review this guide to learn the steps required to properly set up the Cisco Unified IP Phone on the network.

The tasks described are considered to be administration-level tasks and are not intended for end-users of the phones. Many of the tasks involve configuring network settings and affect the phone's ability to function in the network.

Because of the close interaction between the Cisco Unified IP Phone and Cisco Unified Communications Manager, these tasks require familiarity with Cisco Unified Communications Manager.

## Organization

This manual is organized as follows:

Chapter	Description
<a href="#">Chapter 1, “An Overview of the Cisco Unified IP Phone”</a>	Provides a conceptual overview and description of the Cisco Unified IP Phone
<a href="#">Chapter 2, “Preparing to Install the Cisco Unified IP Phone on Your Network”</a>	Describes how the IP Phone interacts with other key IP telephony components, and provides an overview of the tasks required prior to installation
<a href="#">Chapter 3, “Setting Up the Cisco Unified IP Phone”</a>	Describes how to properly and safely install and configure the Cisco Unified IP Phone on your network
<a href="#">Chapter 4, “Configuring Network Settings on the Cisco Unified IP Phone”</a>	Describes how to configure network settings, verify status, and make global changes to the Cisco Unified IP Phone

Chapter	Description
Chapter 5, “Configuring Features, Templates, Services, and Users”	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
Chapter 6, “Viewing Model Information, Status, Statistics, and Security Information on the Cisco Unified IP Phone”	Explains how to view model information, status messages, network statistics, and firmware information from the Cisco Unified IP Phone
Chapter 7, “Monitoring the Cisco Unified IP Phone Remotely”	Explains how to obtain status information about the phone using the phone’s web page
Chapter 8, “Troubleshooting and Maintenance”	Provides tips for troubleshooting the Cisco Unified IP Phone and the Cisco Unified IP Phone Expansion Module 7914
Appendix A, “Providing Information to Users Via a Website”	Provides suggestions for setting up a website for providing users with important information about their Cisco Unified IP Phones
Appendix B, “Feature Support by Protocol for Cisco Unified IP Phone 7960G and 7940G”	Provides information about feature support for the Cisco Unified IP Phone 7960G and 7940G using the SCCP or SIP protocol with Cisco Unified Communications Manager Release 7.0.
Appendix C, “Supporting International Users”	Provides information about setting up phones in non-English environments
Appendix D, “Technical Specifications”	Provides technical specifications of the Cisco Unified IP Phone.
Appendix E, “Basic Phone Administration Steps”	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.

## Related Documentation

For more information about Cisco Unified IP Phones or Cisco Unified Communications Manager, refer to the following publications:

### Cisco Unified IP Phone 7960G/7940G Series

These publications are available at the following URL:

[http://www.cisco.com/en/US/products/hw/phones/ps379/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/hw/phones/ps379/tsd_products_support_series_home.html)

- *Cisco Unified IP Phone 7960G/7940G Series Phone Guide*
- *Cisco Unified IP Phone Features A–Z*
- *Cisco Unified IP Phone Expansion Module 7914 Phone Guide*
- *Installing the Wall Mount Kit for the Cisco Unified IP Phone*
- *Regulatory Compliance and Safety Information for Cisco Unified IP Phones*
- *Open Source License Notices for the Cisco Unified IP Phones 7900 Series*

### Cisco Unified Communications Manager Administration

These publications are available at the following URL:

[http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html)

**Cisco Unified Communications Manager Business Edition**

These publications are available at the following URL:

[http://www.cisco.com/en/US/products/ps7273/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps7273/tsd_products_support_series_home.html)

## Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, 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:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

## 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.access.gpo.gov/bis/ear/ear\\_data.html](http://www.access.gpo.gov/bis/ear/ear_data.html).

## Document Conventions

This document uses the following conventions:

Convention	Description
<b>boldface</b> font	Commands and keywords are in <b>boldface</b> .
<i>italic</i> font	Arguments for which you supply values are in <i>italics</i> .
[ ]	Elements in square brackets are optional.
{ x   y   z }	Alternative keywords are grouped in braces and separated by vertical bars.
[ x   y   z ]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
screen font	Terminal sessions and information the system displays are in <i>screen font</i> .
<b>boldface screen font</b>	Information you must enter is in <b>boldface screen font</b> .
<i>italic screen font</i>	Arguments for which you supply values are in <i>italic screen font</i> .

Convention	Description
^	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.
< >	Nonprinting characters, such as passwords are in angle brackets.

**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.

**Warning**

**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.**



# CHAPTER 1

## An Overview of the Cisco Unified IP Phone

---

The Cisco Unified IP Phone is a full-featured telephone that provides voice communication over an Internet Protocol (IP) network. It functions much like a digital business phone, allowing you to place and receive phone calls and to access features such as mute, hold, transfer, and speed dial. In addition, because the phone is connected to your data network, it offers enhanced IP telephony features, including access to network information and services, and customizable features and services. The phone also supports security features that include file authentication, device authentication, signaling encryption, and media encryption.

This manual describes the Cisco Unified IP Phone 7960G and the Cisco Unified IP Phone 7940G.

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

This chapter includes the following topics:

- [Understanding the Cisco Unified IP Phones 7960G and 7940G, page 1-1](#)
- [What Networking Protocols Are Used?, page 1-4](#)
- [What Features are Supported on the Cisco Unified IP Phones 7960G and 7940G?, page 1-5](#)
- [Understanding Security Features for Cisco Unified IP Phones, page 1-7](#)
- [Overview of Configuring and Installing Cisco Unified IP Phones, page 1-12](#)



### Caution

Using a 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's documentation of the interfering device.

---

## Understanding the Cisco Unified IP Phones 7960G and 7940G

[Figure 1-1](#) shows the main components of the Cisco Unified IP Phone 7960G and [Figure 1-2](#), shows the main components of the Cisco Unified IP Phone 7940G.

These phone models differ only in the number of available line or speed dial buttons. The Cisco Unified IP Phone 7940G has two lines, and the 7960G has six lines.

Figure 1-1 Cisco Unified IP Phone 7960G















77874

Figure 1-2 Cisco Unified IP Phone 7940G



77875

1	Handset light strip	Indicates an incoming call or new voice message.
2	Phone screen	Shows phone features.
3	Model type	Indicates the Cisco Unified IP Phone model.

4	 Programmable buttons	<p>Depending on configuration, programmable buttons provide access to:</p> <ul style="list-style-type: none"> <li>• Phone lines (line buttons)</li> <li>• Speed-dial numbers (speed-dial buttons, including the BLF speed-dial feature)</li> <li>• Web-based services (for example, a Personal Address Book button)</li> <li>• Phone features (for example, a Privacy button)</li> </ul> <p>The Cisco Unified IP Phone 7960G has six programmable buttons and the 7940G has two.</p>
5	Footstand adjustment button	Allows you to adjust the angle of the phone base.
6	 Directories button	Opens/closes the Directories menu. Use it to access call logs and directories.
7	 ? button	Provides access to online Help
8	 Settings button	Opens/closes the Settings menu.
9	 Speaker button	Toggles the speakerphone on or off.
10	 Mute button	Toggles the Mute feature on or off.
11	 Headset button	Toggles the headset on or off.
12	 Volume button	Controls the handset, headset, and speakerphone volume (off-hook) and the ringer volume (on-hook; adjusts contrast settings).
13	 Services button	Opens/closes the Services menu.
14	 Messages button	Auto-dials your voice message service (varies by service).
15	 Navigation button	Allows you to scroll through menus and highlight items. When the phone is on-hook, displays phone numbers from your Placed Calls log.
16	Keypad	Allows you to dial phone numbers, enter letters, and choose menu items.
17	 Softkey buttons	Each activates a softkey option (displayed on your touchscreen).

# What Networking Protocols Are Used?

Cisco Unified IP Phones support several industry-standard and Cisco networking protocols required for voice communication. Table 1-1 provides an overview of the networking protocols that the Cisco Unified IP Phones 7960G and 7940G support.

**Table 1-1 Supported Networking Protocols on the Cisco Unified IP Phone**

Networking Protocol	Purpose	Usage Notes
Bootstrap Protocol (BootP)	BootP enables a network device such as the Cisco Unified IP Phone to discover certain startup information, such as its IP address.	If you are using BootP to assign IP addresses to the Cisco Unified IP Phone, the BOOTP Server option shows “Yes” in the network configuration settings on the phone.
Cisco Discovery Protocol (CDP)	CDP is a device-discovery protocol that runs on all Cisco-manufactured equipment.  Using CDP, a device can advertise its existence to other devices and receive information about other devices in the network.	The Cisco Unified IP Phone uses CDP to communicate information such as auxiliary VLAN ID, per port power management details, and Quality of Service (QoS) configuration information with the Cisco Catalyst switch.
Dynamic Host Configuration Protocol (DHCP)	DHCP dynamically allocates and assigns an IP address to network devices.  DHCP enables you to connect an IP phone into the network and have it become operational without you needing to manually assign an IP address or configure additional required network parameters.	DHCP is enabled by default. If disabled, you must manually configure the IP address, subnet mask, gateway, and a TFTP server on each phone locally.  Cisco recommends that you use DHCP custom option 150. With this method, you configure the TFTP server IP address as the option value. For additional supported DHCP configurations, refer <i>Cisco Unified Communications Manager System Guide</i> .
Hypertext Transfer Protocol (HTTP)	HTTP is the standard way of transferring information and moving documents across the Internet and the web.	Cisco Unified IP Phones use HTTP for the XML services and for troubleshooting purposes.
Internet Protocol (IP)	IP is a messaging protocol that addresses and sends packets across the network.	To communicate using IP, network devices must have an assigned IP address, subnet, and gateway.  IP addresses, subnets, and gateways identifications are automatically assigned if you are using the Cisco Unified IP Phone with Dynamic Host Configuration Protocol (DHCP). If you are not using DHCP, you must manually assign these properties to each phone locally.
Real-Time Transport (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.
Session Initiation Protocol (SIP)	SIP is an emerging standard for setting up telephone calls, multimedia conferencing, and other types of communications on the Internet.	Cisco Unified IP Phones use SCCP for call control. You can configure the Cisco Unified IP Phone to use either SCCP or SIP.



**Table 1-1 Supported Networking Protocols on the Cisco Unified IP Phone (continued)**

Networking Protocol	Purpose	Usage Notes
Skinny Client Control Protocol (SCCP)	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.	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).
Transmission Control Protocol (TCP)	TCP is a connection-oriented transport protocol.	Cisco Unified IP Phones use TCP to connect to Cisco Unified Communications Manager and to access XML services.
Transport Layer Security (TLS)	TLS is a standard protocol for securing and authenticating communications.	When security is implemented, Cisco Unified IP Phones use the TLS protocol when securely registering with Cisco Unified Communications Manager and when communicating with the Certificate Authority Proxy Function (CAPF).
Trivial File Transfer Protocol (TFTP)	TFTP allows you to transfer files over the network.  On the Cisco Unified IP Phone, TFTP enables you to obtain a configuration file specific to the phone type.	TFTP requires a TFTP server in your network, which can be automatically identified from the DHCP server. If you want a phone to use a TFTP server other than the one specified by the DHCP server, you must manually assign the IP address of the TFTP server using the Network Configuration menu on the phone.=
User Datagram Protocol (UDP)	UDP is a connectionless messaging protocol for delivery of data packets.	Cisco Unified IP Phones transmit and receive RTP streams, which utilize UDP.

**Related Topics**

- [Understanding Interactions with Other Cisco Unified IP Communications Products, page 2-2](#)
- [Understanding the Phone Startup Process, page 2-6](#)
- [Network Configuration Menu, page 4-4](#)

## What Features are Supported on the Cisco Unified IP Phones 7960G and 7940G?

The Cisco Unified IP Phones 7960G and 7940G function much like digital business phones, allowing you to place and receive telephone calls. In addition to traditional telephony features, the Cisco Unified IP Phone includes features that enable you to administer and monitor the phone as a network device.

This section covers the following topics:

- [Feature Overview, page 1-6](#)
- [Configuring Telephony Features, page 1-6](#)
- [Configuring Network Parameters Using the Cisco Unified IP Phone, page 1-7](#)
- [Providing Users with Feature Information, page 1-7](#)

## Feature Overview

Cisco Unified IP Phones provide traditional telephony functionality, such as call forwarding and transferring, redialing, speed dialing, conference calling, and voice messaging system access. Cisco Unified IP phones also provide a variety of other features. For an overview of the telephony features that the Cisco Unified IP Phone supports and for tips on configuring them, see the “[Telephony Features Available for the Cisco Unified IP Phone](#)” section on page 5-2.

As with other network devices, you must configure Cisco Unified IP Phones to prepare them to access Cisco Unified Communications Manager and the rest of the IP network. By using DHCP, you have fewer settings to configure on a phone, but if your network requires it, you can manually configure an IP address, TFTP server, and subnet mask. For instructions on configuring the network settings on the Cisco Unified IP Phones, see [Chapter 4, “Configuring Network Settings on the Cisco Unified IP Phone.”](#)

The Cisco Unified IP Phone can interact with other services and devices on your IP network to provide enhanced functionality. For example, you can integrate the Cisco Unified IP Phones with the corporate Lightweight Directory Access Protocol 3 (LDAP3) standard directory to enable users to search for co-worker 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. For information about configuring such services, see the “[Configuring Corporate Directories](#)” section on page 5-9 and the “[Setting Up Services](#)” section on page 5-11.

Finally, because the Cisco Unified IP Phone is a network device, you can obtain detailed status information from it directly. This information can assist you with troubleshooting any problems users might encounter when using their IP phones. See [Chapter 6, “Viewing Model Information, Status, Statistics, and Security Information on the Cisco Unified IP Phone,”](#) for more information.

### Related Topics

- [Configuring Network Settings on the Cisco Unified IP Phone, page 4-1](#)
- [Configuring Features, Templates, Services, and Users, page 5-1](#)
- [Troubleshooting and Maintenance, page 8-1](#)

## Configuring Telephony Features

You can modify additional settings for the Cisco Unified IP Phone 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. See the “[Telephony Features Available for the Cisco Unified IP Phone](#)” section on page 5-2 and refer to the Cisco Unified Communications Manager documentation for additional information.

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

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

[http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod\\_maintenance\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html)

### Related Topic

- [Telephony Features Available for the Cisco Unified IP Phone, page 5-2](#)

## Configuring Network Parameters Using the Cisco Unified IP Phone

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

For more information about configuring features and viewing statistics from the phone, see [Chapter 4, “Configuring Network Settings on the Cisco Unified IP Phone”](#) and see [Chapter 6, “Viewing Model Information, Status, Statistics, and Security Information on the Cisco Unified IP Phone.”](#)

### Related Topics

- [Configuring Network Settings on the Cisco Unified IP Phone, page 4-1](#)
- [Troubleshooting and Maintenance, page 8-1](#)

## Providing Users with Feature Information

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:

[http://www.cisco.com/en/US/products/hw/phones/ps379/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/hw/phones/ps379/tsd_products_support_series_home.html)

From this site, you can view access various user guides.

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

For a summary of some of the key information that phone users need their system administrators to provide, see [Appendix A, “Providing Information to Users Via a Website.”](#)

## Understanding Security Features for Cisco Unified IP Phones

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

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

[Table 1-2](#) shows where you can find additional information about security in this and other documents.



## Overview of Supported Security Features

Table 1-3 provides an overview of the security features that the Cisco Unified IP Phones support. For more information about these features and about Cisco Unified Communications Manager and Cisco Unified IP Phone security, refer to *Cisco Unified Communications Manager Security Guide*.

For information about current security settings on a phone, choose **Settings > Security Configuration**. For more information, see the “[Security Configuration Menu](#)” section on page 6-12.



### Note

Most security features are available only if a certificate trust list (CTL) is installed on the phone. For more information about the CTL, refer to “Configuring the Cisco CTL Client” chapter in *Cisco Unified Communications Manager Security Guide*.

**Table 1-3** Overview of Security Features

Feature	Description
Image authentication	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.
Customer-site certificate installation	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 CAPF. Alternatively, you can install an LSC from the Security Configuration menu on the phone. See the “ <a href="#">Configuring Security on the Cisco Unified IP Phone</a> ” section on page 3-10 for more information.
Device authentication	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 using TLS protocol. Cisco Unified Communications Manager will not register phones unless they can be authenticated by the Cisco Unified Communications Manager.
File authentication	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.
Signaling Authentication	Uses the TLS protocol to validate that no tampering has occurred to signaling packets during transmission.
Manufacturing installed certificate	Each Cisco Unified IP Phone contains a unique manufacturing installed certificate (MIC), which is used for device authentication. The MIC is a permanent unique proof of identity for the phone, and allows Cisco Unified Communications Manager to authenticate the phone.
Secure SRST reference	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.

Table 1-3 Overview of Security Features (continued)

Feature	Description
Media encryption	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.
Signaling Encryption	Ensures that all SCCP signaling messages that are sent between the device and the Cisco Unified Communications Manager server are encrypted.
CAPF (Certificate Authority Proxy Function)	Implements parts of the certificate generation procedure that are too processing-intensive for the phone, and it 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.
Security profiles	Defines whether the phone is nonsecure, authenticated, or encrypted.
Optional disabling of the web server functionality for a phone	You can prevent access to a phone's web page, which displays a variety of operational statistics for the phone.
Phone hardening	<p>Additional security options, which you control from Cisco Unified Communications Manager Administration:</p> <ul style="list-style-type: none"> <li>• Disabling PC port</li> <li>• Disabling Gratuitous ARP (GARP)</li> <li>• Disabling PC Voice VLAN access</li> <li>• Disabling access to the Setting menus, or providing restricted access that allows access to the User Preferences menu and saving volume changes only</li> <li>• Disabling access to web pages for a phone.</li> </ul> <p><b>Note</b> You can view current settings for the PC Port Disabled, GARP Enabled, and Voice VLAN enabled options by looking at the phone's Network Configuration menu. For more information, see the <a href="#">“Displaying the Network Configuration Menu”</a> section on page 4-1.</p>

**Related Topics**

- [Understanding Security Profiles, page 1-10](#)
- [Identifying Encrypted and Authenticated Phone Calls, page 1-11](#)
- [Security Restrictions, page 1-11](#)
- [CAPF Interaction when the Phone Resets, page 1-12](#)

## Understanding Security Profiles

All Cisco Unified IP Phones that support Cisco Unified Communications Manager 7.0 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, refer to *Cisco Unified Communications Manager Security Guide, Release 7.0*.

To view the security mode that is set for the phone, look at the Security Mode setting in the Security Configuration menu. For more information, see the [“Network Configuration Menu”](#) section on page 4-4.

**Related Topics**

- [Identifying Encrypted and Authenticated Phone Calls, page 1-11](#)
- [Security Restrictions, page 1-11](#)

## Identifying Encrypted and Authenticated Phone Calls

When security is implemented for a phone, you can identify authenticated or encrypted phone calls by icons on the screen on the phone.

In an authenticated call, all devices participating in the establishment of the call are authenticated by the Cisco Unified Communications Manager. When a call in progress is authenticated, 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 authenticated by the Cisco Unified Communications Manager. In addition, call signaling and media streams are encrypted. An encrypted call offers the highest 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 non-IP call legs, for example, PSTN, the call may be nonsecure even though it is encrypted within the IP network and has a lock icon associated with it.

**Related Topic**

- [Understanding Security Features for Cisco Unified IP Phones, page 1-7](#)
- [Understanding Security Profiles, page 1-10](#)
- [Security Restrictions, page 1-11](#)

## Security Restrictions

The following restrictions apply to encrypted calls:

- When establishing an encrypted call on a phone that is configured for encryption and associated with a wideband codec region, Cisco Unified Communications Manager ignores the wideband codec and chooses another supported codec from the codec list that the phone presents. If the other devices in the call are not configured for encryption, Cisco Unified Communications Manager may establish the authenticated/nonsecure call by using the wideband codec.
- 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 tone (fast busy tone) plays on the phone on which the user initiated the barge.

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.

## CAPF Interaction when the Phone Resets

The following examples describe how CAPF interacts with the Cisco Unified IP Phone when the phone is reset by a user or by Cisco Unified Communications Manager. In these examples, if an LSC does not already exist in the phone and if By Existing Certificate is selected for the CAPF Authentication Mode, the CAPF certificate operation will fail.

### Example 1

In this example the phone is reset after you configure the Device Security Mode to Nonsecure and the CAPF Authentication Mode to By Null String or By Existing Certificate (Precedence...). After the phone resets, it immediately registers with the primary Cisco Unified Communications Manager and receives the configuration file. The phone then automatically initiates a session with CAPF to download the LSC. After the LSC exists in the phone, configure the Device Support Mode to Authenticated or Encrypted.

### Example 2

In this example, the phone is reset after you configure the Device Security Mode to Authenticated or Encrypted and the CAPF Authentication Mode to By Null String or By Existing Certificate (Precedence...). The phone does not register with the primary Cisco Unified Communications Manager until the CAPF session ends and the phone has installed the LSC. After the session ends, the phone registers and immediately runs in authenticated or encrypted mode.

You cannot configure By Authentication String in this example because the phone will not automatically contact the CAPF server and the registration will fail if the phone does not have a valid LSC.

## Overview of Configuring and Installing Cisco Unified IP Phones

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

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

The following topics provide an overview of procedures for adding Cisco Unified IP Phones to your network:

- [Configuring Cisco Unified IP Phones in Cisco Unified Communications Manager, page 1-13](#)
- [Installing Cisco Unified IP Phones, page 1-16](#)



## Configuring Cisco Unified IP Phones in Cisco Unified Communications Manager

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

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

For more information about these choices, see the [“Adding Phones to the Cisco Unified Communications Manager Database” section on page 2-7](#).

For general information about configuring phones in Cisco Unified Communications Manager, refer to the “Cisco Unified IP Phone” chapter in *Cisco Unified Communications Manager System Guide*.

### Checklist for Configuring the Cisco Unified IP Phone 7960G and 7940G in Cisco Unified Communications Manager

[Table 1-4](#) provides an overview and checklist of configuration tasks for the Cisco Unified IP Phone in Cisco Unified Communications Manager Administration. The list presents 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, refer to the sources in the list.

**Table 1-4 Checklist for Configuring the Cisco Unified IP Phones 7960G and 7940G in Cisco Unified Communications Manager**

Task	Purpose	For More Information
1.	<p>Gather the following information about the phone:</p> <ul style="list-style-type: none"> <li>• Phone Model</li> <li>• MAC address</li> <li>• Physical location of the phone</li> <li>• Name or user ID of phone user</li> <li>• Device pool</li> <li>• Partition, calling search space, and location information</li> <li>• Number of lines and associated directory numbers (DNs) to assign to the phone</li> <li>• Cisco Unified Communications Manager user to associate with the phone</li> <li>• Phone usage information that affects phone button template, softkey template, phone features, IP Phone services, or phone applications</li> </ul> <p>Provides list of configuration requirements for setting up phones.</p> <p>Identifies preliminary configuration that you need to perform before configuring individual phones, such as phone button templates or softkey templates.</p>	<p>Refer to <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phone” chapter.</p> <p>See the <a href="#">“Telephony Features Available for the Cisco Unified IP Phone”</a> section on page 5-2.</p>
2.	<p>Customize phone button templates if required).</p> <p>Changes the number of line buttons, speed-dial buttons, Service URL buttons or adds a Privacy button to meet user needs.</p>	<p>Refer to <i>Cisco Unified Communications Manager Administration Guide</i>, “Phone Button Template Configuration” chapter.</p> <p>See the <a href="#">“Modifying Phone Button Templates”</a> section on page 5-10.</p>
3.	<p>Add and configure the phone by completing the required fields in the Phone Configuration window. Required fields are indicated by an asterisk (*) next to the field name; for example, MAC address and device pool.</p> <p>Adds the device with its default settings to the Cisco Unified Communications Manager database.</p>	<p>Refer to <i>Cisco Unified Communications Manager Administration Guide</i>, “Cisco Unified IP Phone Configuration” chapter.</p> <p>For information about Product Specific Configuration fields, refer to “?” Button Help in the Phone Configuration window.</p>
4.	<p>Add and configure directory numbers (lines) on the phone by completing the required fields in the Directory Number Configuration window. Required fields are indicated by an asterisk (*) next to the field name; for example, directory number and presence group.</p> <p>Adds primary and secondary directory numbers and features associated with directory numbers to the phone.</p>	<p>Refer to the <i>Cisco Unified Communications Manager Administration Guide</i>, Directory Number Configuration chapter, “Creating a Cisco Unity Voice Mailbox” section.</p> <p>See the <a href="#">“Telephony Features Available for the Cisco Unified IP Phone”</a> section on page 5-2.</p>

**Table 1-4 Checklist for Configuring the Cisco Unified IP Phones 7960G and 7940G in Cisco Unified Communications Manager (continued)**

Task	Purpose	For More Information
5.	<p>Customize softkey templates.</p> <p>Adds, deletes, or changes order of softkey features that display on the user's phone to meet feature usage needs.</p>	<p>Refer to <i>Cisco Unified Communications Manager Administration Guide</i>, "Softkey Template Configuration" chapter.</p> <p>See the "Configuring Softkey Templates" section on page 5-11.</p>
6.	<p>Configure speed-dial buttons and assign speed-dial numbers (optional)</p> <p>Adds speed-dial buttons and numbers.</p> <p>Users can change speed-dial settings on their phones by using the Cisco Unified CM User Options.</p>	<p>Refer to <i>Cisco Unified Communications Manager Administration Guide</i>, "Cisco Unified IP Phone Configuration" chapter, "Configuring Speed-Dial Buttons" section.</p>
7.	<p>Configure Cisco Unified IP Phone services and assign services (optional).</p> <p>Provides IP Phone services.</p> <p>Users can add or change services on their phones by using the User Options.</p>	<p>Refer to <i>Cisco Unified Communications Manager Administration Guide</i>, "Cisco Unified IP Phone Services Configuration" chapter.</p> <p>See the "Setting Up Services" section on page 5-11.</p>
8.	<p>Assign services to phone buttons (optional).</p> <p>Provides single button access to an IP phone service or URL.</p>	<p>Refer to <i>Cisco Unified Communications Manager Administration Guide</i>, "Cisco Unified IP Phone Configuration" chapter, "Adding a Cisco Unified IP Phone Service to a Phone Button" section.</p>
9.	<p>Add user information by configuring the required fields:</p> <p><b>Note</b> Assign a password (for the User Options) and PIN (for Extension Mobility and Personal Directory)</p> <p>Adds user information to the global directory for Cisco Unified Communications Manager.</p>	<p>Refer to <i>Cisco Unified Communications Manager Administration Guide</i>, "End User Configuration" chapter.</p> <p>See the "Adding Users to Cisco Unified Communications Manager" section on page 5-12.</p>
10.	<p>Associate a user to a user group.</p> <p>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.</p>	<p>Refer to <i>Cisco Unified Communications Manager Administration Guide</i>:</p> <ul style="list-style-type: none"> <li>• "End User Configuration" chapter, "End User Configuration Settings" section.</li> <li>• "User Group Configuration" chapter, "Adding Users to a User Group" section.</li> </ul>
11.	<p>Associate a user with a phone (optional).</p> <p>Provides users with control over their phone such as forwarding calls or adding speed-dial numbers or services.</p> <p><b>Note</b> Some phones, such as those in conference rooms, do not have an associated user.</p>	<p>Refer to <i>Cisco Unified Communications Manager Administration Guide</i>, "End User Configuration" chapter, "Associating Devices to a User" section.</p>

## Installing Cisco Unified IP Phones

After you have added the phones to the Cisco Unified Communications Manager database, you can complete the phone installation. You (or the phone users) can install the phone at the users's location. The Cisco Unified IP Phone Installation Guide that ships in the box with each phone provides directions for connecting the phone handset, cables, and other accessories.


**Note**

Before you install a phone, even if it is new, upgrade the phone to the current firmware image. For information about upgrading, refer to the Readme file for your phone, which is located at:

<http://www.cisco.com/cgi-bin/tablebuild.pl/ip-7900ser>

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

If you used auto-registration, you need to update the specific configuration information for the phone such as associating the phone with a user, changing the button table, or directory number.

### Checklist for Installing the Cisco Unified IP Phone 7960G and 7940G

Table 1-5 provides an overview and checklist of installation tasks for the Cisco Unified IP Phone 7960G and 7940G. The list presents a suggested order to guide you through the phone installation. Some tasks are optional, depending on your system and user needs. For detailed procedures and information, refer to the sources in the list.

**Table 1-5** Checklist for Installing the Cisco Unified IP Phones 7960G and 7940G

Task	Purpose	For More Information
1.	Choose the power source for the phone: <ul style="list-style-type: none"> <li>• Power over Ethernet (PoE)</li> <li>• External power supply</li> </ul> Determines how the phone receives power.	See the “Providing Power to the Cisco Unified IP Phone” section on page 2-3.
2.	Assemble the phone, adjust phone placement, and connect the network cable. Locates and installs the phone in the network.	See the “Installing the Cisco Unified IP Phone” section on page 3-5. See the “Adjusting the Placement of the Cisco Unified IP Phone” section on page 3-8.
3.	Add a Cisco Unified IP Phone Expansion Module 7914 to the Cisco Unified IP Phone (optional). Extends functionality to a Cisco Unified IP Phone by adding 14 line appearances or speed dial numbers.	See the “Attaching the Cisco Unified IP Phone Expansion Module 7914” section on page 3-7.
4.	Monitor the phone startup process. Verifies that phone is configured properly.	See the “Verifying the Phone Startup Process” section on page 3-9.

Table 1-5 Checklist for Installing the Cisco Unified IP Phones 7960G and 7940G (continued)

Task	Purpose	For More Information
5.	<p>Configure these network settings on the phone by choosing <b>Settings &gt; Network Configuration</b>.</p> <p>Using DHCP—The IP address is automatically assigned and the Cisco Unified IP Phone is directed to a TFTP Server.</p> <p><b>Note</b> Consult with the network administrator if you need to assign an alternative TFTP server instead of using the TFTP server assigned by DHCP.</p> <p>Without DHCP—You must configure the IP address, TFTP server, subnet mask, domain name, and default router locally on the phone.</p> <p>To enable DHCP:</p> <ul style="list-style-type: none"> <li>• Set DHCP Enabled to <b>Yes</b></li> <li>• To use an alternate TFTP server, set Alternate TFTP Server to <b>Yes</b> Enter <b>IP address</b> for TFTP Server 1</li> </ul> <p>To disable DHCP:</p> <ul style="list-style-type: none"> <li>• Set DHCP Enabled to <b>No</b></li> <li>• Enter static <b>IP address</b> for phone</li> <li>• Enter subnet mask</li> <li>• Enter default router IP addresses</li> <li>• Enter domain name where phone resides</li> </ul> <p>Set Alternate TFTP Server to <b>Yes</b> Enter <b>IP address</b> for TFTP Server 1</p>	
6.	<p>Set up security on the phone.</p> <p>Provides protection against data tampering threats and identity theft of phones.</p>	<p>See the <a href="#">“Configuring Security on the Cisco Unified IP Phone”</a> section on page 3-10.</p>
7.	<p>Make calls with the Cisco Unified IP Phone.</p> <p>Verifies that the phone and features work correctly.</p>	<p>Refer to <i>Cisco Unified IP Phone 7960G/7940G Series Phone Guide for Cisco Unified Communications Manager 7.0 (SCCP)</i></p>
8.	<p>Provide information to end users about how to use their phones and how to configure their phone options.</p> <p>Ensures that users have adequate information to successfully use their Cisco Unified IP Phones.</p>	<p>See <a href="#">Appendix A, “Providing Information to Users Via a Website.”</a></p>





## CHAPTER 2

# Preparing to Install the Cisco Unified IP Phone on Your Network

---

Cisco Unified IP Phones enable you to communicate using voice over a data network. To provide this capability, the IP Phones depend upon and interact with several other key Cisco Unified IP Telephony components, including Cisco Unified Communications Manager.

This chapter focuses on the interactions between the Cisco Unified IP Phone 7960G and 7940G and Cisco Unified Communications Manager, DNS and DHCP servers, TFTP servers, and switches. It also describes options for powering phones.

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

<http://www.cisco.com/en/US/products/sw/voicesw/index.html>

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

- [Understanding Interactions with Other Cisco Unified IP Communications Products, page 2-2](#)
- [Providing Power to the Cisco Unified IP Phone, page 2-3](#)
- [Understanding Phone Configuration Files, page 2-5](#)
- [Understanding the Phone Startup Process, page 2-6](#)
- [Adding Phones to the Cisco Unified Communications Manager Database, page 2-7](#)
- [Using Cisco Unified IP Phones with Different Protocols, page 2-10](#)
- [Determining the MAC Address for a Cisco Unified IP Phone, page 2-12](#)

# Understanding Interactions with Other Cisco Unified IP Communications Products

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

This section includes the following topics:

- [Understanding How the Cisco Unified IP Phone Interacts with Cisco Unified Communications Manager, page 2-2](#)
- [Understanding How the Cisco Unified IP Phone Interacts with the VLAN, page 2-3](#)

## Understanding How the Cisco Unified IP Phone Interacts with Cisco Unified Communications Manager

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 IP telephony system—the phones, the access gateways, and the resources necessary for such features as call conferencing and route planning. Cisco Unified Communications Manager also provides:

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

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

For an overview of security functionality for the Cisco Unified IP Phone, see the “[Understanding Security Features for Cisco Unified IP Phones](#)” section on page 1-7.



### Note

If the Cisco Unified IP Phone model that you want to configure does not appear in the Phone Type drop-down list in Cisco Unified Communications Manager Administration, go to the following URL and install the latest support patch for your version of Cisco Unified Communications Manager:  
<http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml>

### Related Topic

- [Telephony Features Available for the Cisco Unified IP Phone, page 5-2](#)



## Understanding How the Cisco Unified IP Phone Interacts with the VLAN

The Cisco Unified IP Phone 7960G and 7940G have an internal Ethernet switch, enabling proper forwarding of appropriate packets to the phone, to the access port (labeled 10/100 PC on the phone), and to the network port (labeled 10/100 SW on the phone).

If a computer is connected to the access port, the computer and the phone share the same physical link to the switch and share the same port on the switch. This shared physical link has the following implications for the VLAN configuration on the network:

- The current VLANs might be configured on an IP subnet basis. However, additional IP addresses might not be available to assign the phone to the same subnet as other devices connected to the same port.
- Data traffic present on the VLAN supporting phones might reduce the quality of Voice-over-IP traffic.
- Network security may indicate a need to isolate the VLAN voice traffic from the VLAN data traffic.

You can resolve these issues by isolating the voice traffic onto a separate VLAN. The switch port that the phone is connected to would be configured to have separate VLANs for carrying:

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

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

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

<http://www.cisco.com/univercd/cc/td/doc/product/lan/index.htm>

### Related Topics

- [Understanding the Phone Startup Process, page 2-6](#)
- [Network and Access Ports, page 3-3](#)
- [Network Configuration Menu, page 4-4](#)

## Providing Power to the Cisco Unified IP Phone

The Cisco Unified IP Phone 7960G and 7940G 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.



### Note

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

These sections provide more information about powering a phone:

- [Power Guidelines, page 2-4](#)
- [Power Outage, page 2-4](#)
- [Obtaining Additional Information about Power, page 2-4](#)

## Power Guidelines

[Table 2-1](#) provides guidelines for powering the Cisco Unified IP Phone 7960G and 7940G.

**Table 2-1 Guidelines for Powering the Cisco Unified IP Phone 7960G and 7940G**

Power Type	Guidelines
External power— Provided through the CP-PWR-CUBE-3 external power supply.	<ul style="list-style-type: none"> <li>• The Cisco Unified IP Phones use the CP-PWR-CUBE-3 power supply.</li> </ul>
PoE power—Provided by a switch through the Ethernet cable attached to the phone.	<ul style="list-style-type: none"> <li>• The Cisco Unified IP Phones support PoE.</li> <li>• The inline power patch panel WS-PWR-PANEL is compatible with the Cisco Unified IP Phones.</li> <li>• To ensure uninterruptible operation of the phone, make sure that the switch has a backup power supply.</li> <li>• 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.</li> </ul>

## Power Outage

Your accessibility to emergency service through the phone is dependent on the phone being powered. If there is an interruption in the power supply, Service and Emergency Calling Service dialing will not function until power is restored. In the case of a power failure or disruption, you may need to reset or reconfigure equipment before using the Service or Emergency Calling Service dialing.

## Obtaining Additional Information about Power

For related information about power, refer to the documents shown in [Table 2-2](#). These documents provide information about the following topics:

- Cisco switches that work with the Cisco Unified IP Phone 7960G and 7940G
- The Cisco IOS releases that support bidirectional power negotiation
- Other requirements and restrictions regarding power


## Understanding Phone Configuration Files

Configuration files for a phone 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 made to the phone's configuration file automatically.

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 files are digitally signed to ensure the authenticity of the files' source.)

In addition, if the device security mode in the configuration file is set to Authenticated and the CTL file on the phone has a valid certificate for Cisco Unified Communications Manager, the phone establishes a TLS connection to Cisco Unified Communications Manager. Otherwise, the phone establishes a TCP connection.



### Note

If the device security mode in the configuration file is set to Authenticated or Encrypted, but the phone has not received a CTL file, the phone will continuously try to obtain a CTL file so that it can register securely.

A phone accesses a default configuration file named `XmlDefault.cnf.xml` from the TFTP server when the following conditions exist:

- You have enabled auto-registration in Cisco Unified Communications Manager
- The phone has not been added to the Cisco Unified Communications Manager Database
- The phone is registering for the first time

If auto registration is not enabled and the phone has not been added to the Cisco Unified Communications Manager Database, the phone registration request will be rejected. In this case, the phone will reset and attempt to register repeatedly.

If the phone has registered before, the phone will access the configuration file named `SEPmac_address.cnf.xml`, where `mac_address` is the MAC address of the phone.

# Understanding the Phone Startup Process

When connecting to the VoIP network, the Cisco Unified IP Phone 7960G and 7940G go through a standard startup process that is described in [Table 2-3](#). Depending on your specific network configuration, not all of these steps may occur on your Cisco Unified IP Phone.

**Table 2-3 Cisco Unified IP Phone 7960G and 7940G Startup Process**

Task	Description	Related Topics
1.	Obtain 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.	<ul style="list-style-type: none"> <li>• <a href="#">Adding Phones to the Cisco Unified Communications Manager Database, page 2-7.</a></li> <li>• <a href="#">Resolving Startup Problems, page 8-1.</a></li> </ul>
2.	Load the stored phone image. The Cisco Unified IP Phone has non-volatile 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.	<a href="#">Resolving Startup Problems, page 8-1.</a>
3.	Configure the VLAN. If the Cisco Unified IP Phone is connected to a Cisco Catalyst switch, the switch next informs the phone of the voice VLAN defined on the switch. The phone needs to know its VLAN membership before it can proceed with the Dynamic Host Configuration Protocol (DHCP) request for an IP address.	<ul style="list-style-type: none"> <li>• <a href="#">Network Configuration Menu, page 4-4.</a></li> <li>• <a href="#">Resolving Startup Problems, page 8-1.</a></li> </ul>
4.	Obtain an IP address. If the Cisco Unified IP Phone is using DHCP to obtain an IP address, the phone queries the DHCP server to obtain one. If you are not using DHCP in your network, you must assign static IP addresses to each phone locally.	<ul style="list-style-type: none"> <li>• <a href="#">Network Configuration Menu, page 4-4.</a></li> <li>• <a href="#">Resolving Startup Problems, page 8-1.</a></li> </ul>
5.	Access a TFTP server. In addition to assigning an IP address, the DHCP server directs the Cisco Unified IP Phone to a TFTP Server. If the phone has a statically-defined IP address, you must configure the TFTP server locally on the phone; the phone then contacts the TFTP server directly.  <b>Note</b> You can also assign an alternative TFTP server to use instead of the one assigned by DHCP.	<ul style="list-style-type: none"> <li>• <a href="#">Network Configuration Menu, page 4-4.</a></li> <li>• <a href="#">Resolving Startup Problems, page 8-1.</a></li> </ul>
6.	Request the CTL file. The TFTP server stores the certificate trust list (CTL) file. This file contains a list of Cisco Unified Communications Managers and TFTP servers that the phone is authorized to connect to. It also contains the certificates necessary for establishing a secure connection between the phone and Cisco Unified Communications Manager.	For more information, refer to the <i>Cisco Unified Communications Manager Security Guide</i>

Table 2-3 Cisco Unified IP Phone 7960G and 7940G Startup Process (continued)

Task	Description	Related Topics
7.	<p>Request the configuration file.</p> <p>The TFTP server has configuration files, which define parameters for connecting to Cisco Unified Communications Manager and other information for the phone.</p>	<ul style="list-style-type: none"> <li>• <a href="#">Adding Phones to the Cisco Unified Communications Manager Database, page 2-7</a></li> <li>• <a href="#">Resolving Startup Problems, page 8-1.</a></li> </ul>
8.	<p>Contact Cisco Unified Communications Manager.</p> <p>The configuration file defines how the Cisco Unified IP Phone communicates with Cisco Unified Communications Manager and provides a phone with its load ID. After obtaining the file from the TFTP server, the phone attempts to make a connection to the highest priority Cisco Unified Communications Manager on the list. If security is implemented, the phone makes a TLS connection. Otherwise, it makes a non-secure TCP connection.</p> <p>If the phone was manually added to the database, Cisco Unified Communications Manager identifies the phone. If the phone was not manually added to the database and auto-registration is enabled in Cisco Unified Communications Manager, the phone attempts to auto-register itself in the Cisco Unified Communications Manager database.</p> <p><b>Note</b> Auto-registration is disabled when security is enabled on Cisco Unified Communications Manager. In this case, the phone must be manually added to the Cisco Unified Communications Manager database.</p>	<p><a href="#">Resolving Startup Problems, page 8-1.</a></p>

## Adding Phones to the Cisco Unified Communications Manager Database

Before installing the Cisco Unified IP phone, you must choose a method for adding phones to the Cisco Unified Communications Manager database. These sections describe the methods:

- [Adding Phones with Auto-Registration, page 2-8](#)
- [Adding Phones with Auto-Registration and TAPS, page 2-9](#)
- [Adding Phones with Cisco Unified Communications Manager Administration, page 2-9](#)
- [Adding Phones with BAT, page 2-10](#)

Table 2-4 provides an overview of these methods for adding phones to the Cisco Unified Communications Manager database.


## Adding Phones with Auto-Registration

By enabling auto-registration before you begin installing phones, you can:

- Automatically add a Cisco Unified IP Phone to the Cisco Unified Communications Manager database when you physically connect the phone to your IP telephony network. During auto-registration, Cisco Unified Communications Manager assigns the next available sequential directory number to the phone.
- Add phones without first gathering MAC addresses from the phones.
- 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 auto-registered phones to new locations and assign them to different device pools without affecting their directory numbers.



### Note

You should use auto-registration to add less than 100 phones to your network. To add more than 100 phones to your network, use the Bulk Administration Tool (BAT). See the [“Adding Phones with BAT” section on page 2-10](#).

In some cases, you might not want to use auto-registration: for example, if you want to assign a specific directory number to the phone or if you plan to implement authentication or encryption, as described in *Cisco Unified Communications Manager Security Guide*. For information about enabling auto-registration, refer to “Enabling Auto-Registration” in *Cisco Unified Communications Manager Administration Guide*.



### Note

Cisco Unified Communications Manager automatically disables auto-registration if you configure the cluster-wide security mode for authentication and encryption through the Cisco CTL client.

### Related Topics

- [Adding Phones with Auto-Registration and TAPS, page 2-9](#)
- [Adding Phones with Cisco Unified Communications Manager Administration, page 2-9](#)
- [Adding Phones with BAT, page 2-10](#)

## Adding Phones with Auto-Registration and TAPS

TAPS, the Tool for Auto-Registered Phones Support, 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. You use TAPS to update MAC addresses and download pre-defined configurations for phones.

You can add phones with auto-registration and TAPS without first gathering MAC addresses from phones.

**Note**

You should use auto-registration 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). See the [“Adding Phones with BAT”](#) section on page 2-10.

To implement TAPS, you or the end-user dial a TAPS directory number and follow voice prompts. When the process is complete, the phone will have downloaded its directory number and other settings, and the phone will be updated in Cisco Unified Communications Manager Administration with the correct MAC address.

Auto-registration must be enabled in Cisco Unified Communications Manager Administration (**System > Cisco Unified CM**) for TAPS to function.

**Note**

Cisco Unified Communications Manager automatically disables auto-registration if you configure the cluster-wide security mode for authentication and encryption through the Cisco CTL client.

Refer to *Cisco Unified Communications Manager Bulk Administration Guide* for detailed instructions about BAT and about TAPS.

**Related Topics**

- [Adding Phones with Auto-Registration, page 2-8](#)
- [Adding Phones with Cisco Unified Communications Manager Administration, page 2-9](#)
- [Adding Phones with BAT, page 2-10](#)

## Adding Phones with Cisco Unified Communications Manager Administration

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.

For information about determining a MAC address, see the [“Determining the MAC Address for a Cisco Unified IP Phone”](#) section on page 2-12.

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, refer to *Cisco Unified Communications Manager Administration Guide* and to *Cisco Unified Communications Manager System Guide*.

**Related Topics**

- [Adding Phones with Auto-Registration, page 2-8](#)
- [Adding Phones with Auto-Registration and TAPS, page 2-9](#)
- [Adding Phones with BAT, page 2-10](#)

## Adding Phones with BAT

The Cisco Bulk Administration Tool (BAT) is a plug-in application for Cisco Unified Communications Manager that enables you to perform batch operations, including registration, on multiple phones.

Before you can add phones using BAT only (not in conjunction with TAPS), you must obtain the MAC address for each phone.

For information about determining a MAC address, see the “[Determining the MAC Address for a Cisco Unified IP Phone](#)” section on page 2-12.

For detailed instructions about using BAT, refer to *Cisco Unified Communications Manager Administration Guide* and to *Cisco Unified Communications Manager Bulk Administration Guide*.

**Related Topics**

- [Adding Phones with Auto-Registration, page 2-8](#)
- [Adding Phones with Auto-Registration and TAPS, page 2-9](#)
- [Adding Phones with Cisco Unified Communications Manager Administration, page 2-9](#)

## Using Cisco Unified IP Phones with Different Protocols

The Cisco Unified IP Phone can operate with SCCP (Skinny Client Control Protocol) or SIP (Session Initiation Protocol). You can convert a phone that is using one protocol for use with the other protocol.

This section includes these topics:

- [Converting a New Phone from SCCP to SIP, page 2-10](#)
- [Converting an In-Use Phone from SCCP to SIP, page 2-11](#)
- [Converting an In-Use Phone from SIP to SCCP, page 2-11](#)
- [Deploying a Phone in an SCCP and SIP Environment, page 2-11](#)

## Converting a 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 auto-register the phone, set the Auto Registration Phone Protocol parameter in Cisco Unified Communications Manager Administration to SIP.
- To provision the phone using the Bulk Administration Tool (BAT), choose the appropriate phone model and choose SIP from the BAT.



- To provision the phone manually, make the appropriate changes for SIP on the Phone Configuration page in Cisco Unified Communications Manager Administration. Refer to *Cisco Unified IP Phone 7960G/7940G Administration Guide for Cisco Unified Communications Manager 7.0 (SIP)*.

Refer to *Cisco Unified Communications Manager Administration Guide* for detailed information about Cisco Unified Communications Manager configuration. Refer to *Cisco Unified Communications Manager Bulk Administration Guide* for detailed information about using the BAT.

- Step 2** If you are not using DHCP in your network, configure the network parameters for the phone.  
See the “Configuring Startup Network Settings” section on page 3-14.
- Step 3** Power cycle the phone.
- 

## Converting an In-Use Phone from SCCP to SIP

You can use the Bulk Administration Tool (BAT) to convert a phone that is in use in your network from SCCP to SIP. To access BAT from Cisco Unified Communications Manager Administration, choose **Bulk Administration > Phones > Migrate Phones > SCCP to SIP**. For detailed information, refer to *Cisco Unified Communications Manager Bulk Administration Guide*.

## Converting an In-Use Phone from SIP to SCCP

To convert a phone that is in use in your network from SIP to SCCP, perform these steps. For more information, *Cisco Unified Communications Manager Administration Guide*.

### Procedure

---

- Step 1** In Cisco Unified Communications Manager Administration, delete the existing SIP phone from the Cisco Unified Communications Manager database.
- Step 2** In Cisco Unified Communications Manager Administration, create the phone as an SCCP phone.
- Step 3** Power cycle the phone.
- 



### Tip

Before deleting a SIP phone (that you want to convert to a SCCP phone) from the Cisco Unified Communications Manager database, copy all of the phone configuration information, so when you add the phone back to the database, you will have the configuration information readily available.

---

## Deploying a Phone in an 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 Auto-Registration parameter is SCCP, perform these general steps:

1. Set the Cisco Unified Communications Manager Auto Registration Protocol enterprise parameter to SCCP.

From Cisco Unified Communications Manager Administration, choose **System > Enterprise Parameters**.

2. Install the phones.
3. Change the Auto Registration Protocol enterprise parameter to SIP.
4. Auto-register the SIP phones.

## Determining the MAC Address for a Cisco Unified IP Phone

Several procedures described in this manual require you to determine the MAC address of a Cisco Unified IP Phone. You can determine a phone's MAC address in these ways:

- From the phone, press the **Settings** button and select **Model Information** and look at the MAC Address field.
- Look at the MAC label on the back of the phone.
- Display the web page for the phone and click the **Device Information** hyperlink.

For information about accessing the web page, see the [“Accessing the Web Page for a Phone”](#) section on page 7-2.



# CHAPTER 3

## Setting Up the Cisco Unified IP Phone

---

This chapter includes the following topics, which help you install the Cisco Unified IP Phone on an IP telephony network:

- [Before You Begin, page 3-1](#)
- [Understanding the Cisco Unified IP Phone 7960G and 7940G Components, page 3-2](#)
- [Installing the Cisco Unified IP Phone, page 3-5](#)
- [Attaching the Cisco Unified IP Phone Expansion Module 7914, page 3-7](#)
- [Adjusting the Placement of the Cisco Unified IP Phone, page 3-8](#)
- [Verifying the Phone Startup Process, page 3-9](#)
- [Configuring Startup Network Settings, page 3-10](#)
- [Configuring Security on the Cisco Unified IP Phone, page 3-10](#)



### 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 [Chapter 2, “Preparing to Install the Cisco Unified IP Phone on Your Network.”](#)

---

## Before You Begin

Before installing the Cisco Unified IP Phone, review the requirements in these sections:

- [Network Requirements, page 3-2](#)
- [Cisco Unified Communications Manager Configuration, page 3-2](#)
- [Understanding the Cisco Unified IP Phone 7960G and 7940G Components, page 3-2](#)

## Network Requirements

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

- Working Voice over IP (VoIP) Network:
  - VoIP configured on your Cisco routers and gateways
  - Cisco Unified Communications Manager installed in your network and configured to handle call processing
- IP network that supports DHCP or manual assignment of IP address, gateway, and subnet mask

The Cisco Unified IP Phone displays the date and time from Cisco Unified Communications Manager. 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 Configuration

The Cisco Unified IP Phone requires Cisco Unified Communications Manager to handle call processing. Refer to *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 auto-registration, verify that it is enabled and properly configured in Cisco Unified Communications Manager before connecting any Cisco Unified IP Phone to the network. See the [“Adding Phones to the Cisco Unified Communications Manager Database”](#) section on page 2-7 for details.

You must use Cisco Unified Communications Manager to configure and assign telephony features to the Cisco Unified IP Phones. See the [“Telephony Features Available for the Cisco Unified IP Phone”](#) section on page 5-2 for details.

In Cisco Unified Communications Manager, you can add users to the database and associate them with specific phones. In this way, users gain access to web pages that allow them to configure phone items such as call forwarding, speed dialing, and voice messaging system options. See the [“Adding Users to Cisco Unified Communications Manager”](#) section on page 5-12 for details.

## Understanding the Cisco Unified IP Phone 7960G and 7940G Components

The Cisco Unified IP Phone 7960G and 7940G includes these components on the phone or as accessories for the phone:

- [Network and Access Ports, page 3-3](#)
- [Handset, page 3-3](#)
- [Speakerphone, page 3-3](#)
- [Headset, page 3-3](#)

## Network and Access Ports

The back of the Cisco Unified IP Phones 7960G and 7940G have two RJ-45 ports labelled 10/100 SW and 10/100 PC. Each port supports 10/100 Mbps half- or full-duplex connections to external devices. You can use either Category 3 or 5 cabling for 10-Mbps connections, but you must use Category 5 for 100 Mbps connections. On both the network port and access port, use full-duplex mode to avoid collisions.

Use the 10/100 SW port to connect the phone to the network. You must use a straight-through cable on these ports. The phone can also obtain inline power from the Cisco Catalyst switch over these connections. See the [“Providing Power to the Cisco Unified IP Phone”](#) section on page 2-3 for details.

Use the 10/100 PC port to connect a network device, such as a computer, to the phone. You must use a straight-through cable on this port.

## Handset

The handset is designed especially for use with a Cisco Unified IP Phone. It includes a light strip that indicates incoming calls and voice messages waiting.

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

## Speakerphone

By default, the speakerphone is enabled on Cisco Unified IP Phones.

You can disable the speakerphone through the Cisco Unified Communications Manager Administration application. To do so, choose **Device > Phone** and locate the phone you want to modify. In the Phone Configuration window for the phone, Product Specific Configuration area, check the **Disable Speakerphone** check box.

## Headset

Although Cisco Systems 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.

In some instances, the mechanics or electronics of various headsets can cause remote parties to hear an echo of their own voice when they speak to Cisco Unified IP Phone users.

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 [Using External Devices with Your Cisco Unified IP Phone](#), page 3-4, 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 en masse.

## Audio Quality Subjective to the User

Beyond the 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 have been reported to perform well with Cisco Unified IP Phones. See manufacturer's sites for details.

## Connecting a Headset

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

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

## Disabling a Headset

You can disable the headset through the Cisco Unified Communications Manager Administration application. If you do so, you also will disable the speakerphone.

To disable the headset from Cisco Unified Communications Manager Administration, choose **Device > Phone** and locate the phone that you want to modify. In the Phone Configuration window for the phone, Product Specific Configuration area, check the **Disable Speakerphone and Headset** check box.

## Using External Devices with Your Cisco Unified IP Phone

The following information applies when you use external devices with the Cisco Unified IP Phone:

Cisco recommends the use of good quality external devices 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 will perform adequately when suitable devices are attached using 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].

## Installing the Cisco Unified IP Phone

You must connect the Cisco Unified IP Phone to the network and to a power source before using it. See [Figure 3-1](#) for a graphical representation of the connections.

**Note**

Before you install a phone, even if it is new, upgrade the phone to the current firmware image. Before using external devices, read the [“Using External Devices with Your Cisco Unified IP Phone”](#) section on [page 3-4](#) for safety and performance information.

**Before You Begin**

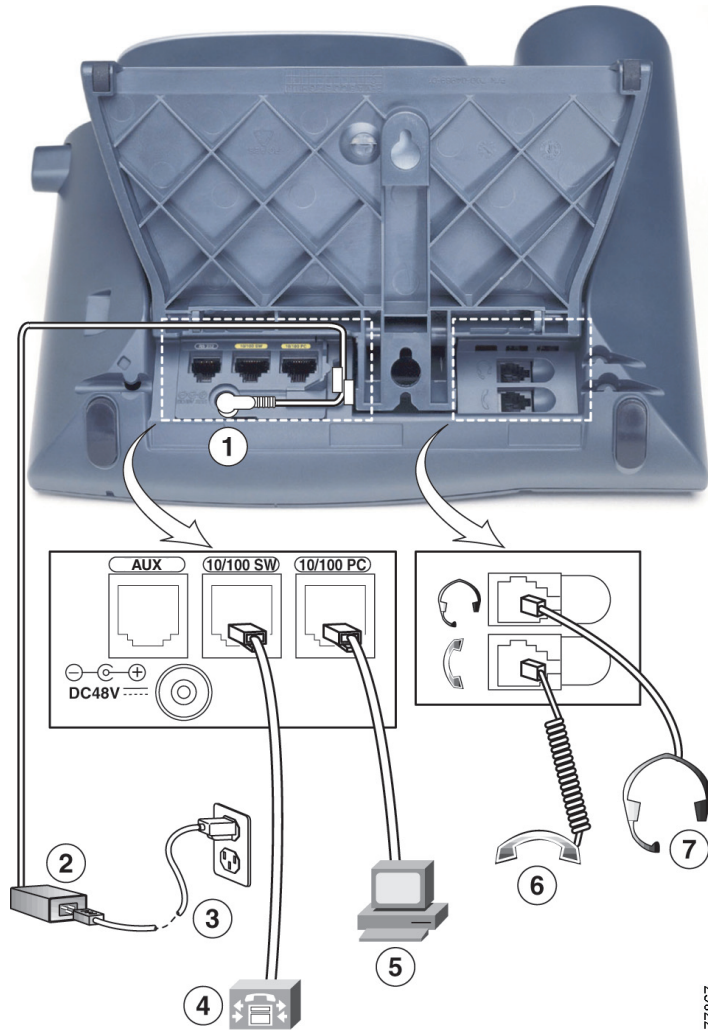
Remove the hookswitch clip (see the [“Handset”](#) section on [page 3-3](#)) from the cradle area.

To install a Cisco Unified IP Phone, perform the following steps:

**Table 3-1** *Installing the Cisco Unified IP Phone 7960G and 7940G*

Task	Procedure	Reference
1.	Connect the handset to the Handset port.	—
2.	Connect a headset to the Headset port. Optional. You can add a headset later if you do not connect one now.	See the <a href="#">“Headset”</a> section on <a href="#">page 3-3</a> for supported headsets.
3.	Connect the power supply to the Cisco DC Adapter port. Optional.	See the <a href="#">“Providing Power to the Cisco Unified IP Phone”</a> section on <a href="#">page 2-3</a> for guidelines.
4.	Connect a Category 3 or 5 straight-through Ethernet cable from the switch to the 10/100 SW port.	See the <a href="#">“Network and Access Ports”</a> section on <a href="#">page 3-3</a> for guidelines.
5.	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.	See the <a href="#">“Network and Access Ports”</a> section on <a href="#">page 3-3</a> for guidelines.

Figure 3-1 Cisco Unified IP Phones 7960G and 7940G Cable Connections



<b>1</b>	DC adaptor port (DC48V) for phones not provided with inline power	<b>5</b>	Access port (10/100 PC) for connecting the phone to a computer
<b>2</b>	AC-to-DC power supply	<b>6</b>	Handset port
<b>3</b>	AC power cord	<b>7</b>	Headset port
<b>4</b>	Network port (10/100 SW) for connecting to the network		

#### Related Topics

- [Attaching the Cisco Unified IP Phone Expansion Module 7914, page 3-7](#)
- [Adjusting the Placement of the Cisco Unified IP Phone, page 3-8](#)
- [Verifying the Phone Startup Process, page 3-9](#)
- [Configuring Startup Network Settings, page 3-10](#)
- [Configuring Security on the Cisco Unified IP Phone, page 3-10](#)



# Attaching the Cisco Unified IP Phone Expansion Module 7914

The Cisco Unified IP Phone Expansion Module 7914 attaches to a Cisco Unified IP Phone 7960G to extend the number or line appearances or programmable buttons on your phone. You can customize the button templates for the Cisco Unified IP Phone Expansion Module 7914 to determine the number of line appearances and speed dial buttons. See the [“Modifying Phone Button Templates”](#) section on [page 5-10](#) for details.

You can attach a Cisco Unified IP Phone Expansion Module 7914 to the Cisco Unified IP Phone 7960G:

- When you initially add the phone to Cisco Unified Communications Manager by selecting **7914 14-Button Line Expansion Module** in the Module 1 or Module 2 fields and selecting the appropriate expansion module firmware. See [Step 6](#) in the following procedure.
- After the phone is configured in Cisco Unified Communications Manager.

To configure the Cisco Unified IP Phone Expansion Module 7914 on the Cisco Unified IP Phone, follow these steps:

## Procedure

- 
- Step 1** Log in to the Cisco Unified Communications Manager Administration application.
- Step 2** From the menu, choose **Device > Phone**.
- The Find and List Phone window displays. You can search for one or more phones that you want to configure for the Cisco Unified IP Phone Expansion Module 7914.
- Step 3** Select and enter your search criteria and click **Find**.
- The Find and List Phone window reopens showing a list of the phones matching your search criteria.
- Step 4** Click the IP Phone that you want to configure for the Cisco Unified IP Phone Expansion Module 7914. The Phone Configuration window displays.
- Step 5** Scroll to the Expansion Module Information section of the window.
- Step 6** To add support for one expansion module, in the Module 1 field, select **7914 14-Button Line Expansion Module**.
- To add support for a second expansion module, in the Module 2 field, select **7914 14-Button Line Expansion Module**.
- In the Firmware Load Information section of the window, there are two fields for specifying the firmware load for Modules 1 and 2. You can leave these fields blank to use the default firmware load.
- Step 7** Scroll to the top of the window and click **Update**.
- A message displays asking you to reset the phone for the changes to take effect. Click **OK**.
- Step 8** Click **Reset Phone** for the changes to take effect.
- 



### Note

Refer users to their Cisco Unified CM User Options web pages so that they can configure speed dial buttons and program buttons to access phone services on the Cisco Unified IP Phone 7914 Expansion Module. See the [“How Users Subscribe to Services and Configure Phone Features”](#) section on [page A-2](#) for more details.

---

**Related Topic**

- [Configuring Softkey Templates, page 5-11](#)

## Adjusting the Placement of the Cisco Unified IP Phone

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

## Adjusting Cisco Unified IP Phone Footstand and Phone Height

You can adjust the footstand adjustment plate on the Cisco Unified IP Phone to the height that provides optimum viewing of the phone screen. See [Figure 3-2](#) for more information.

**Procedure**

- 
- Step 1** Push in the footstand adjustment button.
- Step 2** Adjust the footstand to desired height.
- 

## Mounting the Phone to the Wall

You can mount the Cisco Unified IP Phone on the wall using the footstand as a mounting bracket or you can use special brackets available in a Cisco Unified IP Phone wall mount kit. (Wall mount kits must be ordered separately from the phone.) If you attach the Cisco Unified IP Phone to a wall using the standard footstand and not the wall mount kit, you need to supply the following tools and parts:

- Screwdriver
- Screws to secure the Cisco Unified IP phone to the wall

See [Figure 3-2](#) for a graphical overview of the phone parts.

**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 *Installing the Wall Mount Kit for the Cisco Unified IP Phone*.

**Caution**

---

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

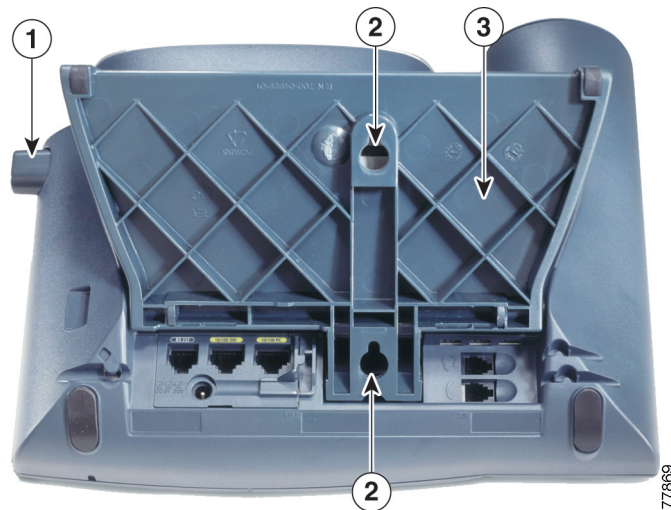
---

**Procedure**

- 
- Step 1** Push in the footstand adjustment button.
- Step 2** Adjust the footstand so it is flat against the back of the phone.

- Step 3** Insert two screws into a wall stud, matching them to the two screw holes on the back of the footstand. The keyholes fit standard phone jack mounts.
- Step 4** Hang the phone on the wall.

**Figure 3-2** Parts Used in Wall Mounting the Cisco Unified IP Phone



<b>1</b>	Footstand adjustment button—Raises and lowers adjustment plate
<b>2</b>	Wall mounting screw holes
<b>3</b>	Adjustment plate—Raises and lowers phone vertically

## Verifying the Phone Startup Process

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

- These buttons flash on and off in sequence:
  - Headset
  - Mute
  - Speaker
- The LCD screen displays the Universal Application Loader screen.
- The LCD screen displays a series of messages that inform you of various activities that the phone performs as it starts up. If the phone upgrades its firmware as part of the startup process, additional messages will inform you about this process.

4. The main LCD screen displays this information:
  - Current date and time
  - Primary 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 the [“Resolving Startup Problems”](#) section on page 8-1.

## Configuring Startup Network Settings

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

- IP address
- IP subnet mask
- Default gateway IP address
- Domain name
- DNS server IP address
- TFTP server IP address

Collect this information and see [Chapter 4, “Configuring Network Settings on the Cisco Unified IP Phone.”](#)

## Configuring Security on the Cisco Unified IP Phone

The security features protects 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 the [“Understanding Security Features for Cisco Unified IP Phones”](#) section on page 1-7. Also, refer to *Cisco Unified Communications Manager Security Guide*.

A Locally Significant Certificate (LSC) installs on phones after you perform the necessary tasks that are associated with the CAPF. You can use Cisco Communications Manager Administration to configure an LSC, as described in *Cisco Unified Communications Manager Security Guide*.

Alternatively, you can initiate the installation of an LSC from the Security Configuration menu on the phone. This menu also lets you update or remove an LSC.

Before you do so, make sure that the appropriate Cisco Unified Communications Manager and the Certificate Authority Proxy Function (CAPF) security configurations are complete:

- The CTL file should have a CAPF certificate.
- The CAPF certificate must exist in the `/usr/local/cm/.security/certs` folder in every server in the cluster.
- The CAPF is running and configured.
- The phone should have the correct load file. To verify the image, choose **Settings > Status > Firmware Versions**. The application load file should begin with P00308.

Refer to *Cisco Unified Communications Manager Security Guide* for more information.

To configure an LSC on the phone, perform these steps:

### Procedure

---

**Step 1** Obtain the CAPF authentication code that was set when the CAPF was configured.

**Step 2** From the phone, choose **Settings > Security Configuration**.



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

---

**Step 3** Press **\*\*#** to unlock settings on the Security Configuration menu.

**Step 4** Scroll to LSC and press the **Update** softkey.

The phone prompts for an authentication string.

**Step 5** Enter the authentication code and press the **Submit** softkey.

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 will display 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 the **Stop** softkey from the Security Configuration menu. (Settings must be unlocked before you can press this softkey.)

When the phone successfully completes the installation procedure, it displays “Success.” If the phone displays, “Failure,” the authorization string may be incorrect or the phone may not be enabled for 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 choosing **Settings > Model Information** and ensuring that the LSC setting shows Yes.

---

### Related Topic

- [Understanding Security Features for Cisco Unified IP Phones, page 1-7](#)





## CHAPTER 4

# Configuring Network Settings on the Cisco Unified IP Phone

---

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 view these settings, and change many of them, through the Network Configuration menu on the phone.

This chapter includes the following topics:

- [Displaying the Network Configuration Menu, page 4-1](#)
- [Unlocking and Locking Options, page 4-2](#)
- [Editing Values, page 4-3](#)
- [Overview of Network Configuration Options, page 4-3](#)
- [Network Configuration Menu, page 4-4](#)

## Displaying the Network Configuration Menu

To display the Network 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. Also prevents handset, speaker, and headset from being saved (but they can be changed temporarily).
- **Restricted**—Prevents access to all options in the Settings menu except Contrast and Ring Type. Allows volume changes to be saved.

If you cannot access an option on the Settings menu, check the Settings Access field. For more information, see *Cisco Unified Communications Manager Administration Guide*.

---

**Procedure**

- 
- Step 1** Press the **Settings** button to access the Settings menu.
- Step 2** Scroll to Network Configuration and press the **Select** softkey.
- 



To exit the Network Configuration menu, press the **Exit** softkey.

**Related Topics**

- [Unlocking and Locking Options, page 4-2](#)
- [Editing Values, page 4-3](#)
- [Overview of Network Configuration Options, page 4-3](#)
- [Network Configuration Menu, page 4-4](#)

## Unlocking and Locking Options

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

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

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

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.

---

**Related Topics**

- [Displaying the Network Configuration Menu, page 4-1](#)
- [Editing Values, page 4-3](#)
- [Overview of Network Configuration Options, page 4-3](#)
- [Network Configuration Menu, page 4-4](#)



## Editing Values

When you edit the value of an option setting on the Network Configuration menu, follow these guidelines:

- Use the keys on the telephone keypad to enter numbers and letters.
- To enter letters using the keypad, use a corresponding number key. Press the key one or more times to display a particular letter. For example, press the 2 key once for “a,” twice quickly for “b,” and three times quickly for “c.” After you pause, the cursor automatically advances to allow you to enter the next letter.
- To enter a period (for example, in an IP address), press the . (period) softkey.
- To correct a mistake, press the << softkey to delete the character to the left of the cursor.
- Press the **Cancel** softkey before pressing the **Validat.** softkey or the **Save** softkey to discard any changes 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 the [“Resetting or Restoring the Cisco Unified IP Phone”](#) section on page 8-13.

### Related Topics

- [Displaying the Network Configuration Menu, page 4-1](#)
- [Unlocking and Locking Options, page 4-2](#)
- [Overview of Network Configuration Options, page 4-3](#)
- [Network Configuration Menu, page 4-4](#)

## Overview of Network Configuration Options

The settings that you can change on a phone’s Network Configuration menu fall into several categories, as shown in [Table 4-1](#). For a detailed explanation of each setting and instructions for changing them, see the [“Network Configuration Menu”](#) section on page 4-4.



### Note

There are several options on the Network 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”](#) section on page 4-4.

**Table 4-1** Settings Configurable from the Network Configuration Menu

Category	Description	Network Configuration Menu Option
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 Enabled
		DHCP Address Released

**Table 4-1** Settings Configurable from the Network Configuration Menu

Category	Description	Network Configuration Menu Option
IP settings	If you do not use DHCP in your network, you can make IP settings manually.	IP Address
		Default Router 1-5
		Subnet Mask
		Domain Name
		DNS Server 1-5
Port settings	Allow you to set the speed and duplex of the network and access ports.	SW Port Configuration
		PC Port Configuration
TFTP settings	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.	TFTP Server 1
		Alternate TFTP Server
		TFTP Server 2
VLAN settings	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.	Admin. VLAN ID
		PC VLAN

**Related Topics**

- [Displaying the Network Configuration Menu, page 4-1](#)
- [Unlocking and Locking Options, page 4-2](#)
- [Editing Values, page 4-3](#)
- [Network Configuration Menu, page 4-4](#)

## Network Configuration Menu

The Network Configuration menu contains options for viewing and making a variety of network settings. [Table 4-2](#) describes these options and, where applicable, explains how to change them.

For information about how to access the Network Configuration menu, see the “[Displaying the Network Configuration Menu](#)” section on page 4-1.

Before you can change an option on this menu, you must unlock options as described in the “[Unlocking and Locking Options](#)” section on page 4-2. The **Edit**, **Yes**, or **No** softkeys for changing network configuration options appear on the Cisco Unified IP Phones 7960G/7940G only if options are unlocked.

For information about the keys you can use to edit options, see the “[Editing Values](#)” section on page 4-3.

**Table 4-2** Network Configuration Menu Options

Option	Description	To Change
DHCP Server	IP address of the Dynamic Host Configuration Protocol (DHCP) server from which the phone obtains its IP address.	Display only—cannot configure.
BOOTP Server	Indicates whether the phone obtains its configuration from a Bootstrap Protocol (BootP) server instead of from a DHCP server.	Display only—cannot configure.

Table 4-2 Network Configuration Menu Options (continued)

Option	Description	To Change
MAC Address	Unique Media Access Control (MAC) address of the phone.	Display only—cannot configure.
Host Name	Unique host name that the DHCP server assigned to the phone.	Display only—cannot configure.
Domain Name	Name of the Domain Name System (DNS) domain in which the phone resides. You can overwrite this value if the Alternate Domain option is set to Yes.	<ol style="list-style-type: none"> <li>1. Set the DHCP Enabled option to No.</li> <li>2. Scroll to the Domain Name option, press the <b>Edit</b> softkey, and then enter a new domain name.</li> <li>3. Press the <b>Validat.</b> softkey and then press the <b>Save</b> softkey.</li> </ol>
IP Address	Internet Protocol (IP) address of the phone. If you assign an IP 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.	<ol style="list-style-type: none"> <li>1. Set the DHCP Enabled option to No.</li> <li>2. Scroll to the IP Address option, press the <b>Edit</b> softkey, and then enter a new IP Address.</li> <li>3. Press the <b>Validat.</b> softkey and then press the <b>Save</b> softkey.</li> </ol>
Subnet Mask	Subnet mask used by the phone.	<ol style="list-style-type: none"> <li>1. Set the DHCP Enabled option to No.</li> <li>2. Scroll to the Subnet Mask option, press the <b>Edit</b> softkey, and then enter a new subnet mask.</li> <li>3. Press the <b>Validat.</b> softkey and then press the <b>Save</b> softkey.</li> </ol>
TFTP Server 1	<p>Primary Trivial File Transfer Protocol (TFTP) server used by the phone. By default this server is CiscoCM1. If you are not using DHCP in your network and you want to change this default server, you must use the TFTP Server 1 option.</p> <p>If you set the Alternate TFTP option to yes, you must enter a non-zero value for the TFTP Server 1 option.</p> <p>If the primary TFTP server is not listed in the CTL file on the phone, you must unlock the CTL file before you can save changes to the TFTP Server 1 option. In this case, the phone will delete the CTL file when you save changes to the TFTP Server 1 option.</p> <p>For information about the CTL file, refer to <i>Cisco Unified Communications Manager Security Guide</i>. For information about unlocking the CTL file, see the “<a href="#">Security Configuration Menu</a>” section on page 6-12.</p>	<ol style="list-style-type: none"> <li>1. Set the Alternate TFTP option to Yes.</li> <li>2. Scroll to the TFTP Server 1 option, press the <b>Edit</b> softkey, and then enter a new TFTP server IP address.</li> <li>3. Press the <b>Validate</b> softkey, and then press the <b>Save</b> softkey.</li> </ol>

Table 4-2 Network Configuration Menu Options (continued)

Option	Description	To Change
Default Router 1 Default Router 2 Default Router 3 Default Router 4 Default Router 5	Default router used by the phone (Default Router 1) and optional backup routers (Default Router 2–5.)	<ol style="list-style-type: none"> <li>1. Set the DHCP Enabled option to No.</li> <li>2. Scroll to the appropriate Default Router option, press the <b>Edit</b> softkey, and then enter a new router IP address.</li> <li>3. Press the <b>Validate</b> softkey.</li> <li>4. Repeat Steps 3 and 4 as needed to assign backup routers.</li> <li>5. Press the <b>Save</b> softkey.</li> </ol>
DNS Server 1 DNS Server 2 DNS Server 3 DNS Server 4 DNS Server 5	Primary Domain Name System (DNS) server (DNS Server 1) and optional backup DNS servers (DNS Server 2–5) used by the phone.	<ol style="list-style-type: none"> <li>1. Scroll to the appropriate DNS Server option, press the <b>Edit</b> softkey, and then enter a new DNS server IP address.</li> <li>2. Press the <b>Validate</b> softkey.</li> <li>3. Repeat Steps 3 and 4 as needed to assign backup DNS servers.</li> <li>4. Press the <b>Save</b> softkey.</li> </ol>
Operational VLAN Id	Auxiliary Virtual Local Area Network (VLAN) configured on a Cisco Catalyst switch in which the phone is a member.  If the phone has not received an auxiliary VLAN, this option indicates the Administrative VLAN.  If neither the auxiliary VLAN nor the Administrative VLAN are configured, this option is blank.	The phone obtains its Operational VLAN Id 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	Auxiliary VLAN in which the phone is a member.  Used only if the phone does not receive an auxiliary VLAN from the switch, ignored otherwise.	<ol style="list-style-type: none"> <li>1. Scroll to the Admin. VLAN Id option, press the <b>Edit</b> softkey, and then enter a new Admin VLAN setting.</li> <li>2. Press the <b>Validate</b> softkey and then press the <b>Save</b> softkey.</li> </ol>
Call Manager 1 Call Manager 2 Call Manager 3 Call Manager 4 Call Manager 5	Cisco Unified Communications Manager servers that are available for processing calls from this phone, in prioritized order.  For more information, see the “ <a href="#">Cisco Unified Communications Manager Options</a> ” section on page 4-10.	You configure an SRST router address in the Cisco Unified Communications Manager Administration SRST Reference Configuration page (choose <b>System &gt; SRST</b> ). You configure an SRST reference in the Device Pool Configuration page (choose <b>System &gt; Device Pool</b> ).
URL Information	URL of the help text that displays on the phone.	From Cisco Unified Communications Manager, choose <b>System &gt; Enterprise Parameters</b> .
URL Directories	URL of the server from which the phone obtains directory information.	From Cisco Unified Communications Manager, choose <b>System &gt; Enterprise Parameters</b> .
URL Messages	URL of the server from which the phone obtains message services.	From Cisco Unified Communications Manager, choose <b>System &gt; Enterprise Parameters</b> .

Table 4-2 Network Configuration Menu Options (continued)

Option	Description	To Change
URL Services	URL of the server from which the phone obtains Cisco Unified IP Phone services.	From Cisco Unified Communications Manager, choose <b>System &gt; Enterprise Parameters</b> .
DHCP Enabled	Indicates whether DHCP is being used by the phone.	<ol style="list-style-type: none"> <li>1. Scroll to the DHCP Enabled option and press the <b>No</b> softkey to disable DHCP, or press the <b>Yes</b> softkey to enable DHCP.</li> <li>2. Press the <b>Save</b> softkey.</li> </ol>
DHCP Address Released	Releases the IP address assigned by DHCP.	<ol style="list-style-type: none"> <li>1. Scroll to the DHCP Address Released option and press the <b>Yes</b> softkey to release the IP address assigned by DHCP, or press the <b>No</b> softkey if you do not want to release this IP address.</li> <li>2. Press the <b>Save</b> softkey.</li> </ol>
Alternate TFTP	Indicates whether the phone is using an alternative TFTP server. If you set this option to Yes, you must enter a value for TFTP Server 1.	<ol style="list-style-type: none"> <li>1. Scroll to the Alternate TFTP option and press the <b>Yes</b> softkey if the phone should use an alternative TFTP server. Press the <b>No</b> softkey otherwise.</li> <li>2. Press the <b>Save</b> softkey.</li> </ol>
Erase Configuration	Changes these settings to their default values: Network Configuration menu settings (including password), Device Configuration menu settings, volume settings, and contrast settings.	<ol style="list-style-type: none"> <li>1. Scroll to the Erase Configuration option and press the <b>Yes</b> softkey</li> <li>2. Press the <b>Save</b> softkey.</li> </ol>
URL Idle	URL that the phone displays when the phone has not been used for the time specified in the Idle URL Time option. For example, you could use the Idle URL option and the Idle URL Timer option to display a log on the LCD screen when the phone has not been used for 5 minutes.	Use Cisco Unified Communications Manager to modify. Choose <b>System &gt; Enterprise Parameters</b> .
URL Idle Time	Amount of time in seconds that elapses before the URL specified in the Idle URL option displays.	From Cisco Unified Communications Manager, choose <b>System &gt; Enterprise Parameters</b> .
URL Authentication	URL that the phone uses to validate requests made to the phone web server.	From Cisco Unified Communications Manager, choose <b>System &gt; Enterprise Parameters</b> .
URL Proxy Server	URL used to proxy HTTP requests for access to non-local host addresses from the phone HTTP client.	From Cisco Unified Communications Manager, choose <b>System &gt; Enterprise Parameters</b> .
PC Port Disabled	Indicates whether the PC port on the phone is enabled (No) or disabled (Yes). Must be set to Yes for video support on the phone.	From Cisco Unified Communications Manager, choose <b>Device &gt; Phone &gt; Phone Configuration</b> .

Table 4-2 Network Configuration Menu Options (continued)

Option	Description	To Change
SW Port Configuration	<p>Speed and duplex of the switch port.</p> <p>If the phone is connected to a switch, you must configure port on the switch to the same speed/duplex as the phone, or configure both to auto-negotiate.</p> <p>If you change the setting of this option, you must change the PC Port Configuration option to the same setting.</p>	<ol style="list-style-type: none"> <li>1. Scroll to the SW Port Configuration option and then press the <b>Edit</b> softkey.</li> <li>2. Enter one of these values: <ul style="list-style-type: none"> <li>– <b>A</b> (Auto Negotiate)</li> <li>– <b>10H</b> (10-BaseT / half duplex)</li> <li>– <b>10F</b> (10-BaseT / full duplex)</li> <li>– <b>100H</b> (100-BaseT / half duplex)</li> <li>– <b>100F</b> (100-BaseT / full duplex)</li> </ul> </li> <li>3. Press press the <b>Save</b> softkey.</li> </ol>
PC Port Configuration	<p>Speed and duplex of the PC port. Valid values:</p> <p>If the phone is connected to a switch, you must configure port on the switch to the same speed/duplex as the phone, or configure both to auto-negotiate.</p> <p>If you change the setting of this option, you must change the SW Port Configuration option to the same setting.</p>	<ol style="list-style-type: none"> <li>1. Scroll to the PC Port Configuration option and then press the <b>Edit</b> softkey.</li> <li>2. Enter one of these values: <ul style="list-style-type: none"> <li>– <b>A</b> (Auto Negotiate)</li> <li>– <b>10H</b> (10-BaseT / half duplex)</li> <li>– <b>10F</b> (10-BaseT / full duplex)</li> <li>– <b>100H</b> (100-BaseT / half duplex)</li> <li>– <b>100F</b> (100-BaseT / full duplex)</li> </ul> </li> <li>3. Press press the <b>Save</b> softkey.</li> </ol>
TFTP Server 2	Optional backup TFTP server that the phone uses if the primary TFTP server is unavailable.	<ol style="list-style-type: none"> <li>1. Set the Alternate TFTP option to Yes.</li> <li>2. Scroll to the TFTP Server 2 option, press the <b>Edit</b> softkey, and then enter a new backup TFTP server IP address.</li> <li>3. Press the <b>Validate</b> softkey, and then press the <b>Save</b> softkey.</li> </ol>
User Locale	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.	From Cisco Unified Communications Manager, choose <b>Device &gt; Phone &gt; Phone Configuration</b> .
Network Locale	Network locale associated with the phone user. The network locale identifies a set of detailed information that supports the phone in a specific location, including definitions of the tones and cadences used by the phone.	From Cisco Unified Communications Manager, choose <b>Device &gt; Phone &gt; Phone Configuration</b> .
User Locale Version	Version of the user locale loaded on the phone.	Display only—cannot configure.
Network Locale Version	Version of the network locale loaded on the phone.	Display only—cannot configure.

**Table 4-2 Network Configuration Menu Options (continued)**

Option	Description	To Change
GARP Enabled	Indicates whether the phone learns MAC addresses from Gratuitous Address Resolution Protocol (ARP) responses. Disabling the phone's ability to accept Gratuitous ARP 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).	From Cisco Unified Communications Manager, choose <b>Device &gt; Phone &gt; Phone Configuration</b> .
Voice VLAN Enabled	Indicates whether the phone allows a device attached to the PC 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. Set this setting 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.	From Cisco Unified Communications Manager, choose <b>Device &gt; Phone &gt; Phone Configuration</b> .
Auto Line Select Enabled	Indicates whether the phone shifts the call focus to incoming calls on all lines. When this option is set to No (disabled), the phone will only shift the call focus to incoming calls on the line that is in use. When this option is set to Yes, the phone will shift the call focus to the line with the most recent incoming call.	From Cisco Unified Communications Manager, choose <b>Device &gt; Phone &gt; Phone Configuration</b> .
Video Capacity Enabled	Indicates whether the phone can participate in video calls when connected to an appropriately equipped PC.	From Cisco Unified Communications Manager, choose <b>Device &gt; Phone &gt; Phone Configuration</b> .
DSCP for Cisco CallManager to Device Interface	Differentiated Services Code Point (DSCP) IP classification for call control signalling.	From Cisco Unified Communications Manager, choose <b>System &gt; Enterprise Parameters</b> .
DSCP For Phone Configuration	DSCP IP classification for any phone configuration transfer.	From Cisco Unified Communications Manager, choose <b>System &gt; Enterprise Parameters</b> .
DSCP For Phone-Based Services	DSCP IP classification for phone-based services.	From Cisco Unified Communications Manager, choose <b>System &gt; Enterprise Parameters</b> .
Security Mode	Displays the security mode that is set for the phone.	From Cisco Unified Communications Manager, choose <b>Device &gt; Phone &gt; Phone Configuration</b> .
Web Access Enabled	Indicates whether the phone's internal web server is enabled (Yes) or disabled (No). When disabled, you cannot access a phone's web pages.	From Cisco Unified Communications Manager, choose <b>Device &gt; Phone &gt; Phone Configuration</b> .

Table 4-2 Network Configuration Menu Options (continued)

Option	Description	To Change
Connection Monitor Duration	Time, in seconds, after a failover that the link between the phone and a Cisco Unified Communications Manager server must remain stable (with no link-flapping) before the phone falls back from SRST to the Cisco Unified Communications Manager server	From Cisco Unified Communications Manager, choose <b>System &gt; Enterprise Parameters</b> .
PC VLAN	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.	<ol style="list-style-type: none"> <li>1. Unlock network configuration options.</li> <li>2. Make sure the Admin VLAN ID option is set.</li> <li>3. Scroll to the <b>PC VLAN</b> option, press the <b>Edit</b> softkey, and then enter a new PC VLAN setting.</li> <li>4. Press the <b>Validate</b> softkey and then press the <b>Save</b> softkey.</li> </ol>

## Cisco Unified Communications Manager Options

The CallManager Configuration menu contains the options Communications Manager 1, Communications Manager 2, Communications Manager 3, Communications Manager 4, and Communications Manager 5. 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, Cisco Unified CM Group Configuration.

For an available Cisco Unified Communications Manager server, an option on the CallManager Configuration menu will show the Cisco Unified Communications Manager server IP address or name and one of the states shown in [Table 4-3](#).

Table 4-3 Cisco Unified Communications Manager Server States

State	Description
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
<i>Blank</i>	No current connection to this Cisco Unified Communications Manager server

An option may also display one of more of the designations or icons shown in [Table 4-4](#):








## CHAPTER 5

# Configuring Features, Templates, Services, and Users

---

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

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

This chapter also explains how you control access to options on the Cisco Unified Communications Manager User Options web pages.

For suggestions about how to provide users with information about features, and what information to provide, see [Appendix A, “Providing Information to Users Via a Website.”](#)

For information about setting up phones in non-English environments, see [Appendix C, “Supporting International Users.”](#)

This chapter includes following topics:

- [Telephony Features Available for the Cisco Unified IP Phone, page 5-2](#)
- [Creating Custom Phone Rings, page 5-9](#)
- [Configuring Corporate and Personal Directories, page 5-9](#)
- [Modifying Phone Button Templates, page 5-10](#)
- [Configuring Softkey Templates, page 5-11](#)
- [Setting Up Services, page 5-11](#)
- [Adding Users to Cisco Unified Communications Manager, page 5-12](#)
- [Managing the User Options Web Pages, page 5-12](#)

# Telephony Features Available for the Cisco Unified IP Phone

After you add Cisco Unified IP Phones to Cisco Unified Communications Manager, you can add functionality to the phones. Table 5-1 includes a list of supported telephony features, many of which you can configure using Cisco Unified Communications Manager Administration. The Reference column lists Cisco Unified Communications Manager and other documentation that contains configuration procedures and related information.

For information about using most of these features on the phone, refer to *Cisco Unified IP Phone 7960G and 7940G Phone Guide*. For a comprehensive listing of features on the phone, refer to *Cisco Unified IP Phone Features A–Z*.


**Note**

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

**Table 5-1** Telephony Features for the Cisco Unified IP Phone

Feature	Description	Configuration Reference
Abbreviated dialing	Allows users to speed dial a phone number by entering an assigned index code (1-99) on the phone keypad.  Users assign index codes from the User Options web pages.	For more information, refer to: <ul style="list-style-type: none"> <li><i>Cisco Unified Communications Manager Administration Guide</i>, “Cisco Unified IP Phone Configuration” chapter.</li> <li><i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phone” chapter.</li> </ul>
Auto Answer	Connects incoming calls automatically after a ring or two.  Auto Answer works with either the speakerphone or headset.	For more information, refer to <i>Cisco Unified Communications Manager Administration Guide</i> , “Directory Number Configuration” chapter.
Auto-pickup	Allows a user to use one-touch, pickup functionality for call pickup, group call pickup, and other group call pickup.	For more information, refer to <i>Cisco Unified Communications Manager Features and Services Guide</i> , “Call Pickup Configuration” chapter.

Table 5-1 Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Barge and (cBarge)	<p>Allows a user to join a non-private call on a shared phone line. Barge features include cBarge and Barge.</p> <ul style="list-style-type: none"> <li>cBarge adds a user to a call and converts it into a conference, allowing the user and other parties to access conference features.</li> <li>Barge adds a user to a call but does not convert the call into a conference.</li> </ul> <p>The phones support Barge in two conference modes:</p> <ul style="list-style-type: none"> <li>Built-in conference bridge at the target device (the phone that is being barged). This mode uses the <b>Barge</b> softkey.</li> <li>Shared conference bridge. This mode uses the <b>cBarge</b> softkey.</li> </ul>	<p>For more information, refer to:</p> <ul style="list-style-type: none"> <li><i>Cisco Unified Communications Manager Administration Guide</i>, “Cisco Unified IP Phone” chapter.</li> <li><i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phones” chapter.</li> <li><i>Cisco Unified Communications Manager Features and Services Guide</i>, “Barge and Privacy” chapter.</li> </ul>
Block external to external transfer	Prevents users from transferring an external call to another external number.	For more information, refer to <i>Cisco Unified Communications Manager Features and Services Guide</i> , “External Call Transfer Restrictions” chapter.
Busy Lamp Field (BLF) speed dial	Allows a user to monitor the call state of a directory number associated with a speed-dial button, call log, or directory listing on the phone.	For more information, refer to <i>Cisco Unified Communications Manager Features and Services Guide</i> , “Presence” chapter.
Call display restrictions	Determines the information that will display for calling or connected lines, depending on the parties who are involved in the call.	<p>For more information, refer to:</p> <ul style="list-style-type: none"> <li><i>Cisco Unified Communications Manager Administration Guide</i>, “Cisco Unified IP Phone Configuration” chapter.</li> <li><i>Cisco Unified Communications Manager System Guide</i>, “Understanding Route Plans” chapter.</li> <li><i>Cisco Unified Communications Manager Features and Services Guide</i>, “Call Display Restrictions” chapter.</li> </ul>
Call Forward	Allows users to redirect incoming calls to another number.	<p>For more information, refer to:</p> <ul style="list-style-type: none"> <li><i>Cisco Unified Communications Manager Administration Guide</i>, “Configuring Directory Numbers” chapter.</li> <li><i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phones” chapter.</li> <li><a href="#">“Specifying Options that Appear on the User Options Web Pages” section on page 5-12</a></li> </ul>
Call park	Allows users to park (temporarily store) a call and then retrieve the call by using another phone in the Cisco Unified Communications Manager system.	For more information, refer to <i>Cisco Unified Communications Manager Features and Services Guide</i> , “Call Park” chapter.

Table 5-1 Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Call pickup	Allows users to redirect a call that is ringing on another phone within their pickup group to their phone.	For more information, refer to <i>Cisco Unified Communications Manager System Guide</i> , “Call Pickup” chapter.
Call waiting	Indicates (and allows users to answer) an incoming call that rings while on another call. Displays incoming call information on the phone screen.	Requires no configuration.
Caller ID	Displays caller identification such as a phone number, name, or other descriptive text on the phone screen.	For more information, refer to: <ul style="list-style-type: none"> <li>• <i>Cisco Unified Communications Manager Administration Guide</i>, “Configuring Cisco Unified IP Phones” chapter.</li> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Understanding Route Plans” chapter.</li> <li>• <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Call Display Restrictions” chapter.</li> </ul>
Call Back	Provides users with an audio and visual alert on the phone when a busy or unavailable party becomes available.	For more information, refer to <i>Cisco Unified Communications Manager Features and Services Guide</i> , “Call Back” chapter.
Conference	<ul style="list-style-type: none"> <li>• Allows a user to talk simultaneously with multiple parties by calling each participant individually. Conference features include Conference, Join, cBarge, and Meet-Me.</li> <li>• 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.</li> </ul>	<ul style="list-style-type: none"> <li>• For more information, refer to <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phones” chapter.</li> <li>• The Service parameter, AdvanceAdhocConference, (disabled by default in Cisco Unified Communications Manager Administration) allows you to enable these features.</li> </ul> <p>For complete information, see the Cisco Unified Communications Manager System Guide, “Conference Bridges” chapter.</p> <p><b>Note</b> Be sure to inform your users whether these features are activated.</p>
Configurable call forward display	Allows you to specify information that appears on a phone when a call is forwarded. This information can include the caller name, caller number, redirected number, and original dialed number.	For more information, refer to: <ul style="list-style-type: none"> <li>• <i>Cisco Unified Communications Manager Administration Guide</i>, “Cisco Unified IP Phone Configuration” chapter.</li> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phones” chapter.</li> </ul>
Direct transfer	Allows users to connect two calls to each other (without remaining on the line).	For more information, refer to <i>Cisco Unified Communications Manager System Guide</i> , “Cisco Unified IP Phones” chapter.

Table 5-1 Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Do Not Disturb (DND)	<p>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.</p> <p>You can configure the phone to have a softkey template with a DND softkey or a phone-button template with DND as one of the selected features.</p> <p>The following DND-related parameters are configurable in Cisco Unified Communications Manager Administration:</p> <ul style="list-style-type: none"> <li>• Do Not Disturb—This check box allows you to enable DND on a per-phone basis. Use Cisco Unified Communications Manager Administration &gt; Device &gt; Phone &gt; Phone Configuration.</li> <li>• 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).</li> <li>• DND Incoming Call Alert—Choose the type of alert to play, if any, on a phone for incoming calls when DND is active. This parameter is located on both the Common Phone Profile window and the Phone configuration window (Phone Configuration window value takes precedence).</li> <li>• BLF Status Depicts DND—Enables DND status to override busy/idle state.</li> </ul>	For information about configuring, refer to <i>Cisco Unified Communications Manager Administration Guide</i> , “Do Not Disturb” chapter.
Extension Mobility Service	<p>Allows a user temporarily to apply a phone number and user profile settings to a shared Cisco Unified IP Phone by logging into the Extension Mobility service on that phone.</p> <p>Extension Mobility can be useful if users work from a variety of locations within your company or if they share a workspace with coworkers.</p>	For more information, refer to <i>Cisco Unified Communications Manager System Guide</i> , “Cisco Unified Communications Manager Extension Mobility and Phone Login Features” chapter.
Group call pickup	Allows a user to answer a call ringing on a phone in another group by using a group pickup code.	For more information, refer to <i>Cisco Unified Communications Manager Features and Services Guide</i> , “Call Pickup” chapter.
Hold/Resume	Allows the user to move a connected call between an active state and a held state.	Requires no configuration, unless you want to use music on hold; see “ <a href="#">Music on hold</a> ” in this table for information.

Table 5-1 Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Immediate Divert	Allows a user to transfer a ringing, connected, or held call directly to a voice-messaging system. When a call is diverted, the line becomes available to make or receive new calls.	For more information, refer to <i>Cisco Unified Communications Manager Features and Services Guide</i> , “Immediate Divert” chapter.
Join/Select	Allows users to join two or more calls that are on one line to create a conference call and remain on the call.	For more information, refer to <i>Cisco Unified Communications Manager System Guide</i> , “Cisco Unified IP Phones” chapter.
Malicious caller identification (MCID)	Allows users to notify the system administrator about suspicious calls that are received.	For more information refer to: <ul style="list-style-type: none"> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phones” chapter.</li> <li>• <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Malicious Call Identification” chapter.</li> </ul>
Meet-Me conference	Allows a user to host a Meet-Me conference in which other participants call a predetermined number at a scheduled time.	For more information refer to <i>Cisco Unified Communications Manager Administration Guide</i> , “Meet-Me Number/Pattern Configuration” chapter.
Message waiting Indicator	A light on the handset that indicates that a user has one or more new voice messages.	For more information refer to: <ul style="list-style-type: none"> <li>• <i>Cisco Unified Communications Manager Administration Guide</i>, “Message Waiting Configuration” chapter.</li> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Voice Mail Connectivity to Cisco Unified Communications Manager” chapter.</li> </ul>
Multilevel Precedence and Preemption (MLPP)	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.	For more information refer to <i>Cisco Unified Communications Manager Features and Services Guide</i> , “Multilevel Precedence and Preemption” chapter.
Music on hold	Plays music while callers are on hold.	For more information refer to <i>Cisco Unified Communications Manager Features and Services Guide</i> , “Music On Hold” chapter.
Onhook call transfer	Allows a user to press a single Transfer softkey and then go onhook to complete a call transfer.	For more information refer to <i>Cisco Unified Communications Manager System Guide</i> , “Cisco Unified IP Phones” chapter.
Other group pickup	Allows a user to answer a call ringing on a phone in another group that is associated with the user's group.	For more information refer to <i>Cisco Unified Communications Manager System Guide</i> , “Call Pickup” chapter.
Presence-enabled directories	Allows a user to monitor the call state of another directory number (DN) listed in call logs, speed-dials, and corporate directories. The Busy Lamp Field (BLF) for the DN displays the call state.	For more information, refer to <i>Cisco Unified Communications Manager Features and Services Guide</i> , “Presence” chapter.



Table 5-1 Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Privacy	Prevents users who share a line from adding themselves to a call and from viewing information on their phone screens about the other user's call.	For more information refer to <i>Cisco Unified Communications Manager Features and Services Guide</i> "Barge and Privacy" chapter.
Quality Reporting Tool (QRT)	Allows users to use the <b>QRT</b> 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 refer to: <ul style="list-style-type: none"> <li><i>Cisco Unified Communications Manager System Guide</i>, "Cisco Unified IP Phones" chapter.</li> <li><i>Cisco Unified Communications Manager Features and Services Guide</i>, "Quality Report Tool" chapter.</li> </ul>
Redial	Allows users to call the most recently dialed phone number by pressing a button.	Requires no configuration.
Ring setting	Identifies ring type used for a line when a phone has another active call.	For more information refer to: <ul style="list-style-type: none"> <li><i>Cisco Unified Communications Manager Administration Guide</i>, "Configuring Directory Numbers" chapter.</li> <li><i>Cisco Unified Communications Manager Features and Services Guide</i>, "Custom Phone Rings" chapter.</li> </ul>
Services	Allows you to use the Cisco Unified IP Phone Services Configuration menu in Cisco Unified Communications Manager Administration to define and maintain the list of phone services to which users can subscribe.	For more information refer to: <ul style="list-style-type: none"> <li><i>Cisco Unified Communications Manager Administration Guide</i>, "Cisco Unified IP Phone Configuration" chapter.</li> <li><i>Cisco Unified Communications Manager System Guide</i>, "Cisco Unified IP Phone Services" chapter.</li> </ul>
Services URL button	Allows users to access services from a programmable button rather than by using the Services menu on a phone.	For more information refer to: <ul style="list-style-type: none"> <li><i>Cisco Unified Communications Manager Administration Guide</i>, "Cisco Unified IP Phone Configuration" chapter.</li> <li><i>Cisco Unified Communications Manager System Guide</i>, "Cisco Unified IP Phone Services" chapter.</li> </ul>
Shared line	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.	For more information refer to <i>Cisco Unified Communications Manager System Guide</i> , "Cisco Unified IP Phones" chapter.
Speed-dialing	Dials a specified number that has been previously stored.	For more information refer to: <ul style="list-style-type: none"> <li><i>Cisco Unified Communications Manager Administration Guide</i>, "Cisco Unified IP Phone Configuration" chapter.</li> <li><i>Cisco Unified Communications Manager System Guide</i>, "Cisco Unified IP Phones" chapter.</li> </ul>

Table 5-1 Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Time-of-Day Routing	Restricts access to specified telephony features by time period.	For more information refer to: <ul style="list-style-type: none"> <li>• <i>Cisco Unified Communications Manager Administration Guide</i>, “Time Period Configuration” chapter.</li> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Time-of-Day Routing” chapter.</li> </ul>
Transfer-direct transfer	<p>Transfer—The first invocation of Transfer will always initiate a new call by using the same directory number, after putting the active call on hold.</p> <p>Direct Transfer—This transfer joins two established calls (call is in hold or in connected state) into one call and drops the feature initiator from the call. Direct Transfer does not initiate a consultation call and does not put the active call on hold.</p>	For more information, refer to the <i>Cisco Unified Communications Manager Administration Guide</i> , “Understanding Directory Numbers” chapter.
Video mode	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: <ul style="list-style-type: none"> <li>• Refer to <i>Cisco Unified Communications Manager Administration Guide</i>, “Conference Bridge Configuration” chapter.</li> <li>• Refer to <i>Cisco Unified Communications Manager System Guide</i>, “Understanding Video Telephony” chapter.</li> </ul>
Video Support	Enable video support on the phone.	For more information refer to: <ul style="list-style-type: none"> <li>• <i>Cisco Unified Communications Manager Administration Guide</i>, “Conference Bridge Configuration” chapter.</li> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Understanding Video Telephony” chapter.</li> <li>• <i>Cisco VT Advantage Administration Guide</i>, “Overview of Cisco VT Advantage” chapter.</li> </ul>
Voice messaging system	Enables callers to leave messages if calls are unanswered.	For more information refer to: <ul style="list-style-type: none"> <li>• <i>Cisco Unified Communications Manager Administration Guide</i>, “Cisco Voice-Mail Port Configuration” chapter.</li> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Voice Mail Connectivity to Cisco Unified Communications Manager” chapter.</li> </ul>

## Creating Custom Phone Rings

You can customize the phone ring types available at your site by using a set of phone ring sounds that are provided by Cisco Unified Communications Manager or by creating your own pulse code modulation (PCM) files and editing the Ringlist.xml file.

Refer to *Cisco Unified Communications Manager Features and Services Guide* for more information.

## Configuring Corporate and Personal Directories

The **Directories** button on the Cisco Unified IP Phones 7960G/7940G 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 the [“Configuring Corporate Directories” section on page 5-9](#) 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 the [“Configuring Personal Directory” section on page 5-9](#) for more information.

### Configuring Corporate Directories

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 the users' rights to access the system. Authorization identifies the telephony resources that a user is permitted to use, such as a specific telephone extension.

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

After the LDAP directory configuration completes, users can use the Corporate Directory service on your Cisco Unified IP Phone 7960G or 7940G to look up users in the corporate directory.

### Configuring Personal Directory

Personal Directory consists of the following features:

- Personal Address Book (PAB)
- Personal Fast Dials (Fast Dials)
- Address Book Synchronization Tool (TABSynch)

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 TABSynch 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 configure Personal Directory from a web browsers, 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 TABSynch utility, provided by you. To obtain the TABSynch software to distribute to users, choose **Application > Plugins** from Cisco Unified Communications Manager Administration, then locate and click **Cisco Unified IP Phone Address Book Synchronizer**.

## Modifying Phone Button Templates

Although the Cisco Unified IP Phones 7960G and 7940G support similar features, each phone model can implement these features differently. Modify phone button templates to assign features to phone buttons and to customize features for a phone model.

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 Administration during registration.

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

The number of buttons and features that you can customize varies based upon Cisco Unified IP Phone model. Familiarize yourself with the configuration options described in [Table 5-2](#).

**Table 5-2 Standard Phone Button Templates Listed by Model**

Cisco Unified IP Phone Model	Standard Phone Button Template Description
Cisco Unified IP Phone 7960G	The standard Cisco Unified IP Phone 7960G template uses buttons 1 and 2 for lines and uses buttons 3 through 6 as speed dials or for access to services. Access other phone features, such as call park, call forward, redial, hold, resume, voice messaging system, conferencing, and so on using softkeys on the Cisco Unified IP Phone 7960G.
Cisco Unified IP Phone 7940G	<p>The Cisco Unified IP Phone 7940G comes with preconfigured phone button templates:</p> <ul style="list-style-type: none"> <li>• 7940G (2-Line)—Uses button 1 and 2 for lines.</li> <li>• 7940G (1-Line)—Uses button 1 for line 1 and button 2 for speed dial.</li> </ul> <p>All Cisco Unified IP Phone 7940G phones use one of these templates.</p> <p>Access phone features, such as call park, call forward, redial, hold, resume, voice messaging system, conferencing, and so on, using softkeys on the Cisco Unified IP Phone 7940G.</p>

# Configuring Softkey Templates

Using Cisco Unified Communications Manager Administration, you can manage softkeys associated with applications that are supported by the Cisco Unified IP Phones 7940G and 7960G.

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

To configure softkey templates, select **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. Refer to *Cisco Unified Communications Manager Administration Guide*, *Cisco Unified Communications Manager System Guide* for more information.

## Setting Up Services

The **Services** button on the Cisco Unified IP Phones 7960G and 7940G gives users access to Cisco Unified IP Phone 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. You can create customized applications for your site.

Before a user can access any service,

- You as the system administrator must use Cisco Unified Communications Manager Administration to configure available services.
- The user must subscribe most to services using the Cisco Unified Communications Manager User Options application. 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 you want to set up and verify that users can access those sites from your corporate IP telephony network.

To set up these services, choose **Device > Device Settings > Phone Services** from Cisco Unified Communications Manager Administration. Refer to *Cisco Unified Communications Manager Administration Guide* and *Cisco Unified Communications Manager System Guide* for more information.

After you configure these services, verify that your users have access to the Cisco Unified Communications Manager IP Phone Options web-based application, from which they can select and subscribe to configured services. See the [“How Users Subscribe to Services and Configure Phone Features” section on page A-2](#) for a summary of the information that you must provide to end users.



### Note

To configure extension mobility services for users, refer to *Cisco Unified Communications Manager Features and Services Guide*.

## Adding Users to Cisco Unified Communications Manager

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

- Access the corporate directory and other customized directories from a Cisco Unified IP Phone
- Create a personal directory
- Set up 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 Management > End User** from Cisco Unified Communications Manager Administration.

Refer to *Cisco Unified Communications Manager Administration Guide* for more information about adding users. Refer to *Cisco Unified Communications Manager System Guide* for details about user information.

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

Refer to *Cisco Unified Communications Manager Bulk Administration Guide* for details.

## Managing the User Options Web Pages

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, refer to *Cisco Unified IP Phone 7960G and 7940G Phone Guide*.

## Giving Users Access to the User Options Web Pages

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 additional information, refer to *Cisco Unified Communications Manager Administration Guide*, “End User Configuration” section.

## Specifying Options that Appear on the User Options Web Pages

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

- Show Ring Settings
- Show Line Text Label Settings
- Show Call Forwarding



### Note

The settings apply to all User Options web pages at your site.

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

### Procedure

---

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

The Enterprise Parameters Configuration window displays.

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

- **True**—Option displays on the User Options web pages (default except for Show Ring Settings, Show Line Text Label, and Show Call Forwarding).
  - **False**—Option does not display on the User Options web pages.
  - **Show All Settings**—All call forward settings display on the User Options web pages (default).
  - **Hide All Settings**—No call forward settings display on the User Options web pages.
  - **Show Only Call Forward All**—Only call forward all calls displays on the User Options web pages.
-







## CHAPTER 6

# Viewing Model Information, Status, Statistics, and Security Information on the Cisco Unified IP Phone

---

This chapter describes how to access and use the following menus and screens on the Cisco Unified IP Phone:

- Model Information screen—Displays hardware and software information about the phone.
- Status menu—Provides access to screens that display the status messages, network statistics, and firmware versions.
- Call Statistics screen—Displays counters and statistics for the current call.
- Security Configuration menu—Displays information about security on the phone and provides access to the CTL File menu and to the Trust List menu.

You can use the information on these screens to monitor the operation of a phone and to assist with troubleshooting. In addition, from the CTL File menu, you can unlock and remove the CTL file from the phone.

You can also obtain much of this information, and obtain other related information, remotely through a phone's web page. For more information, see [Chapter 7, “Monitoring the Cisco Unified IP Phone Remotely.”](#)

For more information about troubleshooting, see [Chapter 8, “Troubleshooting and Maintenance.”](#)

This chapter includes these topics:

- [Model Information Screen, page 6-2](#)
- [Status Menu, page 6-2](#)
- [Call Statistics Screen, page 6-10.](#)
- [Security Configuration Menu, page 6-12](#)

## Model Information Screen

The Model Information screen displays this information:

- Model Number—Model number of the phone.
- MAC Address—MAC address of the phone.
- APP Load ID—Identifies the JAR file running on the phone.
- Boot Load ID—Identifies the factory-installed load running on the phone.
- Serial Number—Serial number of the phone.
- Load File—Identifies the factory-installed load running on the phone.
- CTL—Displays the MD5 hash of the certificate trust list (CTL) file that is installed in the phone. If no CTL file is installed on the phone, this field displays No. (The CTL file installs automatically when the phone reboots or resets. For more information about this file, refer to *Cisco Unified Communications Manager Security Guide*.)
- MIC—Indicates whether a manufacturing installed certificate (used for the security features) is installed on the phone.
- LSC—Indicates whether a locally significant certificate (used for the security features) is installed on the phone.

To display the Model Information menu, press the **Settings** button and then select **Model Information**.

To exit the Model Information menu, press the **Exit** softkey.

## Status Menu

The Status menu includes these options, which provide information about the phone and its operation:

- Status Messages—Displays the Status Messages screen, which shows a log of important system messages. For more information, see the “[Status Messages Screen](#)” section on page 6-3.
- Network Statistics—Displays the Network Statistics screen, which shows Ethernet traffic statistics. For more information, see the “[Network Statistics Screen](#)” section on page 6-7.
- Firmware Versions—Displays the Firmware Versions screen, which shows information about the firmware running on the phone. For more information, see the “[Firmware Versions Screen](#)” section on page 6-8.
- Expansion Module Stats—Displays the Expansion Module Stats screen, which shows information about the Cisco Unified IP Phone Expansion Module 7914, if connected to the phone. For more information, see the “[Expansion Module Stats Screen](#)” section on page 6-9.

To display the Status menu, press the **Settings** button and then select **Status**.

To exit the Status menu, press the **Exit** softkey.

## Status Messages Screen

You can access the Status Messages screen at any time, even if the phone has not finished starting up. [Table 6-1](#) describes the status messages that might appear. This table also includes actions you can take to address errors that are indicated.

To display the Status Messages screen, follow these steps:

### Procedure

- 
- Step 1** Press the **Settings** button.
- Step 2** Select **Status**.
- Step 3** Select **Status Messages**.
- 

To exit the Status Messages screen, press the **Exit** softkey.

**Table 6-1** Status Messages on the Cisco Unified IP Phones 7960G and 7940G

Message	Description	Possible Explanation and Action
BootP server used	The phone obtained its IP address from a BootP server rather than a DHCP server.	None. This message is informational only.
File auth error	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.	<ul style="list-style-type: none"> <li>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.</li> <li>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.</li> </ul>

Table 6-1 Status Messages on the Cisco Unified IP Phones 7960G and 7940G (continued)

Message	Description	Possible Explanation and Action
CFG file not found	The name-based and default configuration file was not found on the TFTP Server.	<p>The configuration file for a phone is created when the phone is added to the Cisco Unified Communications Manager database. If the phone has not been added to the Cisco Unified Communications Manager database, the TFTP server generates a <code>CFG File Not Found</code> response.</p> <ul style="list-style-type: none"> <li>Phone is not registered with Cisco Unified Communications Manager.</li> </ul> <p>You must manually add the phone to Cisco Unified Communications Manager if you are not allowing phones to auto-register. See the <a href="#">“Adding Phones with Cisco Unified Communications Manager Administration”</a> section on page 2-9 for details.</p> <ul style="list-style-type: none"> <li>If you are using DHCP, verify that the DHCP server is pointing to the correct TFTP server.</li> <li>If you are using static IP addresses, check configuration of the TFTP server. See the <a href="#">“Network Configuration Menu”</a> section on page 4-4 for details on assigning a TFTP server.</li> </ul>
CFG TFTP Size Error	The configuration file is too large for file system on the phone.	Power cycle the phone.
Checksum Error	Downloaded software file is corrupted.	Obtain a new copy of the phone firmware and place it in the <code>TFTPath</code> directory. You should only copy files into this directory when the TFTP server software is shut down, otherwise the files may be corrupted.
DHCP timeout	DHCP server did not respond.	<ul style="list-style-type: none"> <li>Network is busy—The errors should resolve themselves when the network load reduces.</li> <li>No network connectivity between the DHCP server and the phone—Verify the network connections.</li> <li>DHCP server is down—Check configuration of DHCP server.</li> <li>Errors persist—Consider assigning a static IP address. See the <a href="#">“Network Configuration Menu”</a> section on page 4-4 for details on assigning a static IP address.</li> </ul>

**Table 6-1** Status Messages on the Cisco Unified IP Phones 7960G and 7940G (continued)

Message	Description	Possible Explanation and Action
DNS timeout	DNS server did not respond.	<ul style="list-style-type: none"> <li>• Network is busy—The errors should resolve themselves when the network load reduces.</li> <li>• No network connectivity between the DNS server and the phone—Verify the network connections.</li> <li>• DNS server is down—Check configuration of DNS server.</li> </ul>
DNS unknown host	DNS could not resolve the name of the TFTP server or Cisco Unified Communications Manager.	<ul style="list-style-type: none"> <li>• Verify that the host names of the TFTP server or Cisco Unified Communications Manager are configured properly in DNS.</li> <li>• Consider using IP addresses rather than host names.</li> </ul>
Duplicate IP	Another device is using the IP address assigned to the phone.	<ul style="list-style-type: none"> <li>• If the phone has a static IP address, verify that you have not assigned a duplicate IP address. See the “<a href="#">Network Configuration Menu</a>” section on page 4-4 section for details</li> <li>• If you are using DHCP, check the DHCP server configuration.</li> </ul>
Error update locale	One or more localization files could not be found in the TFTPPath directory or were not valid. The locale was not changed.	<p>From Cisco Unified Operating System Administration, check that the following files are located within the subdirectories in TFTP File Management.</p> <ul style="list-style-type: none"> <li>• Located in subdirectory with same name as network locale: <ul style="list-style-type: none"> <li>– tones.xml</li> </ul> </li> <li>• Located in subdirectory with same name as user locale: <ul style="list-style-type: none"> <li>– glyphs.xml</li> <li>– dictionary.xml</li> <li>– kate.xml</li> </ul> </li> </ul>
IP address released	The phone has been configured to release its IP address.	The phone remains idle until it is power cycled or you reset the DHCP address. See the “ <a href="#">Network Configuration Menu</a> ” section on page 4-4 section for details.
Load ID incorrect	Load ID of the software file is of the wrong type.	Check the load ID assigned to the phone (from Cisco Unified Communications Manager, choose <b>Device &gt; Phone</b> ). Verify that the load ID is entered correctly.

Table 6-1 Status Messages on the Cisco Unified IP Phones 7960G and 7940G (continued)

Message	Description	Possible Explanation and Action
Load rejected HC	The application that was downloaded is not compatible with the phone's hardware.	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 <b>Device &gt; Phone</b> ). Re-enter the load displayed on the phone. See the " <a href="#">Firmware Versions Screen</a> " section on <a href="#">page 6-8</a> to verify the phone setting.
No default router	DHCP or static configuration did not specify a default router.	<ul style="list-style-type: none"> <li>If the phone has a static IP address, verify that the default router has been configured. See the "<a href="#">Network Configuration Menu</a>" section on <a href="#">page 4-4</a> section for details.</li> <li>If you are using DHCP, the DHCP server has not provided a default router. Check the DHCP server configuration.</li> </ul>
No DNS server IP	A name was specified but DHCP or static IP configuration did not specify a DNS server address.	<ul style="list-style-type: none"> <li>If the phone has a static IP address, verify that the DNS server has been configured. See the "<a href="#">Network Configuration Menu</a>" section on <a href="#">page 4-4</a> section for details.</li> <li>If you are using DHCP, the DHCP server has not provided a DNS server. Check the DHCP server configuration.</li> </ul>
Programming Error	The phone failed during programming.	Attempt to resolve this error by power cycling the phone. If the problem persists, contact Cisco technical support for additional assistance.
XmlDefault.cnf.xml, or .cnf.xml 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.
TFTP access error	TFTP server is pointing to a directory that does not exist.	<ul style="list-style-type: none"> <li>If you are using DHCP, verify that the DHCP server is pointing to the correct TFTP server.</li> <li>If you are using static IP addresses, check configuration of TFTP server. See the "<a href="#">Network Configuration Menu</a>" section on <a href="#">page 4-4</a> for details on assigning a TFTP server.</li> </ul>
TFTP file not found	The requested load file (.bin) was not found in the TFTPPath directory.	From Cisco Unified Operating System Administration, make sure that the phone load file is listed in TFTP File Management.

**Table 6-1** Status Messages on the Cisco Unified IP Phones 7960G and 7940G (continued)

Message	Description	Possible Explanation and Action
TFTP server not authorized	The specified TFTP server could not be found in the phone's CTL.	<ul style="list-style-type: none"> <li>The DHCP server is not configured properly and is not serving the correct TFTP server address. In this case, update the TFTP server configuration to specify the correct TFTP server.</li> <li>If the phone is using a static IP address, the phone may be configured with the wrong TFTP server address. In this case, enter the correct TFTP server address in the Network Configuration menu on the phone.</li> <li>If the TFTP server address is correct, there may be a problem with the CTL file. In this case, run the CTL client and update the CTL file, making sure that the proper TFTP servers are included in this file.</li> </ul>
TFTP timeout	TFTP server did not respond.	<ul style="list-style-type: none"> <li>Network is busy—The errors should resolve themselves when the network load reduces.</li> <li>No network connectivity between the TFTP server and the phone—Verify the network connections.</li> <li>TFTP server is down—Check configuration of TFTP server.</li> </ul>

## Network Statistics Screen

The Network Statistics displays information about the phone and network performance. [Table 6-2](#) explains components of text messages that might appear in this screen.

To display the Network Statistics screen, follow these steps:

### Procedure

- 
- Step 1** Press the **Settings** button.
- Step 2** Select **Status**.
- Step 3** Select **Network Statistics**.
- 

To exit the Network Statistics screen, press the **Exit** softkey.

**Table 6-2** Network Statistics Message Components

Message Component	Description
Rcv Frames	Number of packets received by the phone
Xmt	Number of packets transmitted by the phone
REr	Number of error packets received by the phone

**Table 6-2 Network Statistics Message Components (continued)**

Message Component	Description
Bcast	Number of broadcast packets received by the phone
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 reset of the phone
Elapsed Time	Amount of time that has elapsed since the phone last rebooted
Port 1	Link state and connection of the PC port (for example, <code>Auto 100 Mb Full-Duplex</code> means that the PC port is in a link up state and has auto-negotiated a full-duplex, 100-Mbps connection)
Port 2	Link state and connection of the Network port

## Firmware Versions Screen

The Firmware Versions screen displays the following information about the firmware running on the phone:

- App Load ID—Version of the phone application running on the phone
- Boot Load ID—Identifier of the factory-installed load running on the phone
- Version—Version of the firmware running on the phone
- DSP—Identifies the digital signal processor (DSP) software version used
- Expansion Module 1, Expansion Module 2—Identifies the load running on the Expansion Module or Expansion Modules, if connected to the phone



To display the Firmware Version screen, follow these steps:

#### Procedure

- 
- Step 1** Press the **Settings** button.
  - Step 2** Select **Status**.
  - Step 3** Select **Firmware Versions**.
- 

To exit the Firmware Version screen, press the **Exit** softkey.

## Expansion Module Stats Screen

The Expansion Module Stats screen displays information about each Cisco Unified IP Phone Expansion Module 7914 that is connected to the phone.

Table 6-3 explains the information that is displayed on this screen for each connected expansion module. You can use this information to troubleshoot the expansion module, if necessary. In the Expansion Module Stats screen, a statistic preceded by “A” is for the first expansion module. A statistic preceded by “B” is for the second expansion module.

To display the Expansion Module Stats screen, follow these steps:

#### Procedure

- 
- Step 1** Press the **Settings** button.
  - Step 2** Select **Status**.
  - Step 3** Select **Expansion Module Stats**.
- 

To exit the Expansion Module Stats screen, press the **Exit** softkey.

**Table 6-3** Expansion Module Statistics

Item	Description
Link State	Overall expansion module status
RX Discarded Bytes	Number of bytes discarded due to errors
RX Length Err	Number of packets discarded due to improper length
RX Checksum Err	Number of packets discarded due to invalid checksum information
RX Invalid Message	Number of packets that have been discarded because a message was invalid or unsupported
TX Retransmit	Number of packets that have been retransmitted to the expansion module
TX Buffer Full	Number of packets discarded because the expansion module was not able to accept new messages

# Call Statistics Screen

The Call Statistics screen displays counters statistics and voice quality metrics in these ways:

- During call—You can view the call information by pressing the ? button twice rapidly.
- After the 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. For more information about remote monitoring, see [Chapter 7, “Monitoring the Cisco Unified IP Phone Remotely.”](#)

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.

To display the Call Statistics screen for information about the last voice stream, follow these steps:

## Procedure

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

To exit the Call Statistics Screen screen, press the **Exit** softkey.

The Call Statistics Screen displays the items shown in [6-4](#).

**Table 6-4 Call Statistics Items**

Item	Description
RxType	Type of voice stream received (RTP streaming audio): G.729, G.711 u-law, G.711 A-law, or Lin16k.
RxSize	Size of voice packets, in milliseconds, in the receiving voice stream (RTP streaming audio).
RxCnt	Number of RTP voice packets received since voice stream was opened. <b>Note</b> This number is not necessarily identical to the number of RTP voice packets received since the call began because the call might have been placed on hold.
TxSize	Size of voice packets, in milliseconds, in the transmitting voice stream.
TxCnt	Number of RTP voice packets transmitted since voice stream was opened. <b>Note</b> This number is not necessarily identical to the number of RTP voice packets transmitted since the call began because the call might have been placed on hold.

**Table 6-4 Call Statistics Items (continued)**

Item	Description
Avg Jtr	Estimated average RTP packet jitter (dynamic delay that a packet encounters when going through the network) observed since the receiving voice stream was opened.
Max Jtr	Maximum jitter observed since the receiving voice stream was opened.
RxDisc	Number of RTP packets in the receiving voice stream that have been discarded (bad packets, too late, and so on).  <b>Note</b> The phone will discard payload type 19 comfort noise packets that are generated by Cisco Gateways, which will increment this counter.
RxLost	Missing RTP packets (lost in transit).
<b>Voice Quality Metrics</b>	
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 the <a href="#">“Monitoring the Voice Quality of Calls”</a> section on page 8-15.  <b>Note</b> 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: <ul style="list-style-type: none"> <li>• G.711 gives 4.5</li> <li>• G.729 A /AB gives 3.7</li> </ul>
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.

## Security Configuration Menu

The Security Configuration menu displays information about security on the phone and provides access to the CTL File menu and to the Trust List menu. The Security Configuration menu contains these options:

- **Web Access**—Indicates whether web access is enabled or disabled for the phone. You configure web access with Cisco Unified Communications Manager Administration.
- **Security Mode**—Displays the security mode that is set for the phone. You configure the security mode in Cisco Unified Communications Manager Administration.
- **MIC**—Indicates whether a manufacturing installed certificate is installed on the phone.
- **LSC**—Indicates whether a locally significant certificate is installed on the phone.

Also lets you enter an authorization string for an LSC. For more information, see the [“Configuring Security on the Cisco Unified IP Phone”](#) section on page 3-10.

- **CTL File**—If a CTL file is installed on the phone, provides access to the CTL File menu. A locked padlock icon in this option indicates that the CTL file is locked. An unlocked padlock icon indicates that the CTL file is unlocked. If a CTL file is not installed on the phone, this option displays Not Installed. For more information, see the [“CTL File Menu”](#) section on page 6-12.
- **Trust List**—If a CTL file is installed on the phone, provides access to the Trust List menu. For more information, see the [“Trust List Menu”](#) section on page 6-14.
- **CAPF**—Displays the IP address and the port of the CAPF server that the phone uses.

To display the Security Configuration menu, press the **Settings** button and then select **Security Configuration**.

To exit the Security Configuration menu, press the **Exit** softkey.

## CTL File Menu

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

To exit the CTL File menu, press the **Exit** softkey.

The CTL File menu contains these options:

- **CTL File**—Displays the MD5 hash of the certificate trust list (CTL) file that is installed in the phone. (If security is configured for the phone, the CTL file installs automatically when the phone reboots or resets. For more information about this file, refer to *Cisco Unified Communications Manager Security Guide*.) Also lets you unlock the CTL file and remove it from the phone.

A locked padlock icon in this option indicates that the CTL file is locked. An unlocked padlock icon indicates that the CTL file is unlocked.

- **Call Manager/ TFPT**—IP address 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 (see [Figure 6-1](#)).
- **CAPF**—IP address of the CAPF server used by the phone. Also displays a certificate icon if a certificate is installed for this server.

- Communications Manager—IP address of the Cisco Unified Communications Manager server used by the phone. Also displays a certificate icon if a certificate is installed for this server (see [Figure 6-1](#)).
- TFTP Server—IP address of a TFTP server used by the phone. Also displays a certificate icon if a certificate is installed for this server (see [Figure 6-1](#)).

**Figure 6-1 Certificate Icon**



If the primary TFTP server (TFTP Server 1) or the backup TFTP server (TFTP Server 2) is not listed in the CTL file, you must unlock the CTL file before you can save changes that you make to the TFTP Server 1 option on the Network Configuration menu. (For information about changing this option, see the [“Network Configuration Menu” section on page 4-4](#).)

To unlock the CTL file and change the TFTP Server 1 option or remove the CTL file, follow these steps:

#### Procedure

- 
- Step 1** Press **\*\*#** to unlock options on the Security Configuration menu.
- For detailed information about unlocking options, see the [“Unlocking and Locking Options” section on page 4-2](#).
- Step 2** Pressing the **Settings** button and choose **Security Configuration > CTL File**.
- The CTL File menu displays.
- Step 3** Highlight the CTL option.
- Step 4** Press the **Unlock** softkey to unlock the CTL file.
- Step 5** Take one of these actions:
- Change the TFTP Server 1 option on the Network Configuration menu.  
When you save your changes, the CTL file is locked again automatically.
  - Press the **Erase** softkey to remove the CTL file from the phone.  
The CTL file is removed and the phone resets.



---

**Note** When you press the **Unlock** softkey, it changes to **Lock**. If you decide not to change the TFTP Server 1 option or not to erase the CTL file, press the **Lock** softkey to lock the CTL file.

---

## Trust List Menu

The Trust List menu displays information about all of the servers that the phone trusts.

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

To exit the Trust List menu, press the **Exit** softkey.

The Trust List menu contains these options:

- Communications Manager / TFTP—IP address of a trusted Cisco Unified Communications Manager and TFTP server used by the phone. Also displays a certificate icon if a certificate is installed for this server (see [Figure 6-1](#)).
- CAPF—IP address of the trusted CAPF server used by the phone. Also displays a certificate icon if a certificate is installed for this server (see [Figure 6-1](#)).
- Communications Manager—IP address of the trusted Cisco Unified Communications Manager server used by the phone. Also displays a certificate icon if a certificate is installed for this server (see [Figure 6-1](#)).
- SRST—IP address 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 device (see [Figure 6-1](#)).
- TFTP Server—IP address of a TFTP server used by the phone. Also displays a certificate icon if a certificate is installed for this server (see [Figure 6-1](#)).



## CHAPTER 7

# Monitoring the Cisco Unified IP Phone Remotely

---

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

This chapter describes the information that you can obtain from the phone's 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 [Chapter 6, “Viewing Model Information, Status, Statistics, and Security Information on the Cisco Unified IP Phone.”](#)

For more information about troubleshooting the Cisco Unified IP Phone, [Chapter 8, “Troubleshooting and Maintenance.”](#)

This chapter includes these topics:

- [Accessing the Web Page for a Phone, page 7-2](#)
- [Disabling and Enabling Web Page Access, page 7-3](#)
- [Device Information, page 7-3](#)
- [Network Configuration, page 7-4](#)
- [Network Statistics, page 7-7](#)
- [Device Logs, page 7-10](#)
- [Streaming Statistics, page 7-11](#)

# Accessing the Web Page for a Phone

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



## Note

If you cannot access the web page, it may be disabled. See the [“Disabling and Enabling Web Page Access” section on page 7-3](#) 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 on the Find and List Phones web page and at the top of the Phone Configuration web page.
  - On the Cisco Unified IP Phone, press the **Settings** button, choose **Network Configuration**, and then scroll to the IP Address option.
- Step 2** Open a web browser and enter the following URL, where *IP\_address* is the IP address of the Cisco Unified IP Phone:
- `http://IP_address`
- 

The web page for a Cisco Unified IP Phone includes these topics:

- **Device Information**—Displays device settings and related information for the phone. For more information, see the [“Device Information” section on page 7-3](#).
- **Network Configuration**—Displays network configuration information and information about other phone settings. For more information, see the [“Network Configuration” section on page 7-4](#).
- **Network Statistics**—Includes the following hyperlinks, which provide information about network traffic:
  - **Ethernet**—Displays information about Ethernet traffic. For more information, see the [“Network Statistics” section on page 7-7](#).
  - **Port 1 (Network)**—Displays information about network traffic to and from the 10/100 SW port on the phone. This port connects the phone to the network. For more information, see the [“Network Statistics” section on page 7-7](#).
  - **Port 2 (Access)**—Displays information about network traffic to and from the 10/100 PC port on the phone. This port connects the phone to a network device, such as a computer. For more information, see the [“Network Statistics” section on page 7-7](#).
  - **Port 3 (Phone)**—Displays information about network traffic to and from the phone. For more information, see the [“Network Statistics” section on page 7-7](#).
- **Device Logs**—Includes the following hyperlinks, which provide information that you can use for troubleshooting:
  - **Debug Display**—provides information that may be useful to the Cisco TAC if you require assistance with troubleshooting
  - **Stack Statistics**—Displays information about the phone’s stack tasks. For more information, see the [“Device Logs” section on page 7-10](#).



- **Status Messages**—Displays various system messages. For more information, see the “[Device Logs](#)” section on page 7-10.
- **Streaming Statistics**—Includes the following hyperlink:
  - **Stream 1**—Display a variety of streaming statistics. For more information, see the “[Streaming Statistics](#)” section on page 7-11.

## Disabling and Enabling Web Page Access

For security purposes, you may choose to prevent access to the web pages for a phone. If you do so, you will prevent access to the web pages that are described in this chapter and to the Cisco Unified CM User Options.

To disable access to the web pages for a phone, follow these steps from Cisco Unified Communications Manager Administration:

- 
- 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 **Disabled**.
- Step 5** Click **Update**.




---

**Note** Some features, such as Cisco Quality Report Tool, do not function properly without access to the phone web pages. Disabling web access also affects any serviceability application that relies on web access, such as CiscoWorks.

---

To enable web page access when it is disabled, see the preceding steps about disabling access. Follow the same steps, but choose **Enabled** in [Step 4](#) to enable the web page.

## Device Information

The Device Information area on a phone’s web page displays device settings and related information for the phone. [Table 7-1](#) describes these items.

To display the Device Information area, access the web page for the phone as described in the “[Accessing the Web Page for a Phone](#)” section on page 7-2, and then click the **Device Information** hyperlink.

**Table 7-1** *Device Information Area Items*

Item	Description
MAC Address	Media Access Control (MAC) address of the phone
Host Name	Host name that the DHCP server assigned to the phone
Phone DN	Directory number assigned to the phone
App Load ID	Identifier of the firmware running on the phone

**Table 7-1** Device Information Area Items (continued)

Item	Description
Boot Load ID	Identifier of the factory-installed load running on the phone
Version	Version of the phone hardware
Expansion Module 1	Phone load ID for the first Cisco Unified IP Phone Expansion Module 7914, if connected to the phone
Expansion Module 2	Phone load ID for the second Cisco Unified IP Phone Expansion Module 7914, if connected to the phone
Hardware Revision	Version of the phone hardware
Serial Number	Serial number of the phone
Model Number	Model number of the phone
Codec	Codec used by the phone
Amps	Indicates whether 3 volt or 5 volt amplifier is being used by the phone
C3PO Revision	Revision of the Cisco 3 port switch in the phone
Message Waiting	Indicates if there is a voice message waiting on any line for this phone

## Network Configuration

The Network Configuration area on a phone's web page displays network configuration information and information about other phone settings. [Table 7-2](#) describes these items.

You can view and set many of these items from the Network Configuration Menu the Cisco Unified IP Phone. For more information, see [Chapter 4, "Configuring Network Settings on the Cisco Unified IP Phone."](#)

To display the Network Configuration area, access the web page for the phone as described in the ["Accessing the Web Page for a Phone"](#) section on page 7-2, and then click the **Network Configuration** hyperlink.

**Table 7-2** Network Configuration Area Items

Item	Description
DHCP Server	IP address of the Dynamic Host Configuration Protocol (DHCP) server from which the phone obtains its IP address.
BOOTP Server	Indicates whether the phone obtains its configuration from a Bootstrap Protocol (BootP) server.
MAC Address	Media Access Control (MAC) address of the phone.
Host Name	Host name that the DHCP server assigned to the phone.
Domain Name	Name of the Domain Name System (DNS) domain in which the phone resides.
IP Address	Internet Protocol (IP) address of the phone.
Subnet Mask	Subnet mask used by the phone.
TFTP Server 1	Primary Trivial File Transfer Protocol (TFTP) server used by the phone.

**Table 7-2 Network Configuration Area Items (continued)**

Item	Description
Default Router 1–5	Default router used by the phone (Default Router 1) and optional backup routers (Default Router 2–5).
DNS Server 1–5	Primary Domain Name System (DNS) server (DNS Server 1) and optional backup DNS servers (DNS Server 2–5) used by the phone.
VLAN ID	Auxiliary Virtual Local Area Network (VLAN) configured on a Cisco Catalyst switch in which the phone is a member.
Admin. VLAN Id	Auxiliary VLAN in which the phone is a member.
Call Manager 1–5	<p>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.</p> <p>For an available server, an item will show the Cisco Unified Communications Manager server IP address and one of the following states:</p> <ul style="list-style-type: none"> <li>• Active—Cisco Unified Communications Manager server from which the phone is currently receiving call-processing services.</li> <li>• Standby—Cisco Unified Communications Manager server to which the phone switches if the current server becomes unavailable.</li> <li>• Blank—No current connection to this Cisco Unified Communications Manager server.</li> </ul> <p>An item may also include the Survivable Remote Site Telephony (SRST) designation, which identifies an SRST router capable of providing Cisco Unified Communications Manager functionality with a limited feature set. This router assumes control of call processing if all other Cisco Unified Communications Manager servers become unreachable. The SRST Cisco Unified Communications Manager always appears last in the list of servers, even if it is active.</p> <p>An item will include a shield icon if the phone has an authenticated connection to the Cisco Unified Communications Manager server. It will display a padlock icon if the phone has an authenticated connection to the Cisco Unified Communications Manager server.</p>
Information URL	URL of the help text that appears on the phone.
Directories URL	URL of the server from which the phone obtains directory information.
Messages URL	URL of the server from which the phone obtains message services.
Services URL	URL of the server from which the phone obtains Cisco Unified IP Phone services.
DHCP Enabled	Indicates whether DHCP is being used by the phone.
DHCP Address Released	Indicates the setting of the DHCP Address Released option on the phone's Network Configuration menu.
Alternate TFTP	Indicates whether the phone is using an alternative TFTP server.
Erase Configuration	Indicates the setting of the Erase Configuration option on the phone's Network Configuration menu.

**Table 7-2 Network Configuration Area Items (continued)**

<b>Item</b>	<b>Description</b>
Idle URL	URL that the phone displays when the phone has not been used for the time specified by Idle URL Time.
Idle URL Time	Amount of time in seconds that elapses before the URL shown in Idle URL appears.
Authentication URL	URL that the phone uses to validate requests made to the phone web server.
Proxy Server URL	URL used to proxy HTTP requests for access to non-local host addresses from the phone HTTP client.
PC Port Disabled	Indicates whether the PC port on the phone is enabled or disabled.
SW Port Configuration	Speed and duplex of the switch port, where: <ul style="list-style-type: none"> <li>• A—Auto Negotiate</li> <li>• 10H—10-BaseT / half duplex</li> <li>• 10F—10-BaseT / full duplex</li> <li>• 100H—100-BaseT / half duplex</li> <li>• 100F—100-BaseT / full duplex</li> <li>• No Link—No connection to the switch port</li> </ul>
PC Port Configuration	Speed and duplex of the switch port, where: <ul style="list-style-type: none"> <li>• A—Auto Negotiate</li> <li>• 10H—10-BaseT / half duplex</li> <li>• 10F—10-BaseT / full duplex</li> <li>• 100H—100-BaseT / half duplex</li> <li>• 100F—100-BaseT / full duplex</li> <li>• No Link—No connection to the PC port</li> </ul>
TFTP Server 2	Backup TFTP server that the phone uses if the primary TFTP server is unavailable.
User Locale	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.
Network Locale	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.
Handset Only Mode	Indicates whether the speakerphone and headset are enabled (No) or disabled (Yes) on the phone. When the speakerphone and headset are disabled, the phone will function with the handset only.
User Locale Version	Version of the user locale loaded on the phone.
Network Locale Version	Version of the network locale loaded on the phone.
GARP Enabled	Indicates whether the phone learns MAC addresses from Gratuitous ARP responses.

**Table 7-2** Network Configuration Area Items (continued)

Item	Description
Voice VLAN Enabled	Indicates whether the phone allows a device attached to the PC port to access the Voice VLAN.
Auto Line Select Enabled	Indicates whether the phone shifts the call focus to incoming calls on all lines.
Video Capability Enabled	Indicates whether the phone can participate in video calls when connected to an appropriately equipped PC.

## Network Statistics

These Network Statistics areas on a phone's web page provide information about network traffic on the phone:

- Ethernet area—Displays information about Ethernet traffic. See the “[Ethernet Statistics](#)” section on [page 7-7](#) for detailed information. [Table 7-3](#) describes the items in this area.
- Port 1 (Network) area—Displays information about network traffic to and from the 10/100 SW port on the phone. See the “[Port 1 \(Network\), Port 2 \(Access\), and Port 3 \(Phone\) Statistics](#)” section on [page 7-8](#) for detailed information.
- Port 2 (Access)—Displays information about network traffic to and from the 10/100 PC port on the phone. See the “[Port 1 \(Network\), Port 2 \(Access\), and Port 3 \(Phone\) Statistics](#)” section on [page 7-8](#) for detailed information.
- Port 3 (Phone)—Displays information about network traffic to and from the phone. See the “[Port 1 \(Network\), Port 2 \(Access\), and Port 3 \(Phone\) Statistics](#)” section on [page 7-8](#) for detailed information.

To display a Network Statistics area, access the web page for the phone as described in the “[Accessing the Web Page for a Phone](#)” section on [page 7-2](#), and then click the **Ethernet Information**, the **Access**, or the **Network** hyperlink.

## Ethernet Statistics

The Ethernet area on a phone's web page provides detailed information about Ethernet traffic to and from the phone.

To display this area, access the web page for the phone as described in the “[Accessing the Web Page for a Phone](#)” section on [page 7-2](#), and then click the **Ethernet** hyperlink.

[Table 7-3](#) describes the items in the Ethernet Statistics area.

**Table 7-3** Ethernet Area Items

Item	Description
Tx Excessive Collisions	Indicates whether packets are being lost because of network congestion
Tx Frames	Total number of packets transmitted by the phone
Tx Broadcasts	Total number of broadcast packets transmitted by the phone
Tx Multicasts	Total number of multicast packets transmitted by the phone

**Table 7-3 Ethernet Area Items (continued)**

Item	Description
Tx Collisions	Total number of collisions that occurred while a packet was being transmitted
Tx Deferred Abort	Total number of transmit packets aborted by the phone
Rx Overruns	Total number of received packets dropped because of buffer overruns
Rx Long/CRC	Total number of received packets dropped because of excessive length
Rx Frames	Total number of packets received by the phone
Rx CRC Errors	Total number of received packets dropped because of invalid CRC information
Rx Bad Preamble	Total number of received packets dropped because of bad Ethernet preamble information
Rx Runt	Total number of received packets dropped because of insufficient length
Rx Multicasts	Total number of multicast packets received by the phone
Rx Broadcasts	Total number of broadcast packets received by the phone
Rx Shorts	Total number of good packets received that are less than 64 bytes size
Rx Longs	Total number of good packets received that are greater than 1522 bytes in size

## Port 1 (Network), Port 2 (Access), and Port 3 (Phone) Statistics

The following area on a phone's web page provide information about network traffic to and from ports on the phone:

- Port 1 (Network)—Provides information about the 10/100 SW port
- Port 2 (Access)—Provides information about the 10/100 PC port
- Port 3 (Phone)—Provides information about network traffic to and from the phone

To display any of these areas, access the web page for the phone as described in the [“Accessing the Web Page for a Phone”](#) section on page 7-2, and then click the **Port 1 (Network)**, the **Port 2 (Access)**, or the **Port 3 (Phone)** hyperlink.

[Table 7-4](#) describes the items in the Port 1 (Network), Port 2 (Access), and Port 3 (Phone) areas.

**Table 7-4 Port Statistics Area Items**

Item	Description
Carrier Events	Indicates loss of carrier on the port
Rx totalPkt	Total number of packets received by the phone
Rx crcErr	Total number of packets received with CRC failed
Rx alignErr	Total number of packets received between 64 and 1522 bytes in length that have a bad FCS
Rx multicast	Total number of multicast packets received by the phone
Rx broadcast	Total number of broadcast packets received by the phone

**Table 7-4 Port Statistics Area Items (continued)**

<b>Item</b>	<b>Description</b>
Rx unicast	Total number of unicast packets received by the phone
Rx shortErr	Total number of FCS error packets or Align error packets received that are less than 64 bytes in size
Rx shortGood	Total number of good packets received that are less than 64 bytes size
Rx longGood	Total number of good packets received that are greater than 1522 bytes in size
Rx longErr	Total number of FCS error packets or Align error packets received that are greater than 1522 bytes in size
Rx size64	Total number of packets received, including bad packets, that are between 0 and 64 bytes in size
Rx size65to127	Total number of packets received, including bad packets, that are between 65 and 127 bytes in size
Rx size128to255	Total number of packets received, including bad packets, that are between 128 and 255 bytes in size
Rx size256to511	Total number of packets received, including bad packets, that are between 256 and 511 bytes in size
Rx size512to1023	Total number of packets received, including bad packets, that are between 512 and 1023 bytes in size
Rx size1024to1518	Total number of packets received, including bad packets, that are between 1024 and 1518 bytes in size
Rx size1519to1548	Total number of packets received, including bad packets, that are between 1519 and 1548 bytes in size
Rx tokenDrop	Total number of packets dropped due to lack of resources (for example, FIFO overflow)
Tx excessDefer	Total number of packets delayed from transmitting due to medium being busy
Tx lateCollision	Number of times that collisions occurred later than 512 bit times after the start of packet transmission
Tx totalGoodPkt	Total number of good packets (multicast, broadcast, and unicast) received by the phone
Tx Collisions	Total number of collisions that occurred while a packet was being transmitted
Tx fifoUnderrun	Total number of transmitted packets dropped because of FIFO underrun
Tx excessLength	Total number of packets not transmitted because the packet experienced 16 transmission attempts
Tx broadcast	Total number of broadcast packets transmitted by the phone
Tx multicast	Total number of multicast packets transmitted by the phone
Tx size64	Total number of packets transmitted, including bad packets, that are between 0 and 64 bytes in size
Tx size65to127	Total number of packets transmitted, including bad packets, that are between 65 and 127 bytes in size
Tx size128to255	Total number of packets transmitted, including bad packets, that are between 128 and 255 bytes in size

**Table 7-4 Port Statistics Area Items (continued)**

Item	Description
Tx size256to511	Total number of packets transmitted, including bad packets, that are between 256 and 511 bytes in size
Tx size512to1023	Total number of packets transmitted, including bad packets, that are between 512 and 1023 bytes in size
Tx size1024to1518	Total number of packets received, including bad packets, that are between 1024 and 1518 bytes in size
cos 0 Drop	Total number of packets with Class of Service 0 dropped because of threshold checking
cos 1 Drop	Total number of packets with Class of Service 1 dropped because of threshold checking
cos 2 Drop	Total number of packets with Class of Service 2 dropped because of threshold checking
cos 3 Drop	Total number of packets with Class of Service 3 dropped because of threshold checking
cos 4 Drop	Total number of packets with Class of Service 4 dropped because of threshold checking
cos 5 Drop	Total number of packets with Class of Service 5 dropped because of threshold checking
cos 6 Drop	Total number of packets with Class of Service 6 dropped because of threshold checking
cos 7 Drop	Total number of packets with Class of Service 7 dropped because of threshold checking
bpdu Drop	Total number of Bridge Protocol Data Unit frames dropped because of threshold checking
overflow Drop	Total number of packets dropped because of an internal queue overflow
Neighbor Device ID	Identifier of a device connected to this port
Neighbor IP Address	IP address of the neighbor device
Neighbor Port	Neighbor device port to which the phone is connected

## Device Logs

The Device Logs area on a phone's web page provide information you can use to help monitor and troubleshoot the phone:

- Debug Display area—Provides information that may be useful to the Cisco TAC if you require assistance with troubleshooting.
- Stack Statistics area—Displays information about the phone's stack tasks. See the [“Stack Statistics” section on page 7-11](#) for detailed information.
- Status Messages area—Displays up to the 10 most recent status messages that the phone has generated since it was last powered up. See the [“Status Messages” section on page 7-11](#) for detailed information.



## Stack Statistics

The Debug Display area on a phone's web page displays information about the phone's stack tasks. This information may be useful to Cisco Technical Assistance Center personnel if you require assistance with troubleshooting.

To display the Stack Statistics area, access the web page for the phone as described in the [“Accessing the Web Page for a Phone”](#) section on page 7-2, and then click the **Stack Statistics** hyperlink.

Table 7-5 describes the items in the Stack Statistics area.

**Table 7-5**      **Stack Statistics Area Items**

Item	Description
Socket Task	Peak stack consumption for the Socket task
Phone Task	Peak stack consumption for the Phone task
DSPPoll Task	Peak stack consumption for the DPPoll task
RTP Task	Peak stack consumption for the RTP task
TLS Task	Peak stack consumption for the TLS task
Config Task	Peak stack consumption for the Config task
Display Task	Peak stack consumption for the Display task
CAST Task	Peak stack consumption for the CAST task
Sidecar Task	Peak stack consumption for the Sidecar task
Audit Task	Peak stack consumption for the Socket task
Undefined Mode	Peak stack consumption for the undefined mode
SVC Mode	Peak stack consumption for the SVC mode
IRQ Mode	Peak stack consumption for the IRQ mode
FIQ Mode	Peak stack consumption for the FIQ mode
SYS Mode	Peak stack consumption for the SYS mode

## Status Messages

The Status Messages area on a phone's web page 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. Table 6-1 describes the status messages that can appear.

## Streaming Statistics

A phone streams information when it is on a call or running a service that sends or receives audio or data. The Stream 1 area on a phone's web page provides information about this stream. Table 7-6 describes the items in this area.

To display a network statistics area, access the web page for the phone as described in the [“Accessing the Web Page for a Phone”](#) section on page 7-2, and then click the **Stream 1** hyperlink.

**Table 7-6 Streaming Statistics Area Items**

Item	Description
Domain	Domain of the phone
Remote Address	IP address of the destination of the stream
Local Address	IP address of the phone
Sender Joins	Number of times the phone has started transmitting a stream
Receiver Joins	Number of times the phone has started receiving a stream
Byes	Number of times the phone has stopped transmitting a stream
Start Time	Internal time stamp indicating when Cisco Unified Communications Manager requested that the phone start transmitting packets
Row Status	Whether the phone is streaming
Host Name	Host name of the phone
Sender Packets	Total number of packets sent by the phone
Sender Octets	Total number of octets sent by the phone
Sender Tool	Type of audio encoding used for the stream
Sender Reports	Number of times this streaming statistics report has been accessed from the web page (resets when the phone resets)
Sender Report Time	Internal time stamp indicating when this streaming statistics report was generated
Sender Start Time	Time that the stream started
Rcvr Lost Packets	Total number of packets lost
Rcvr Jitter	Maximum jitter of stream
Receiver Tool	Type of audio encoding used for the stream
Rcvr Reports	Number of times this streaming statistics report has been accessed from the web page (resets when the phone resets)
Rcvr Report Time	Internal time stamp indicating when this streaming statistics report was generated
Rcvr Packets	Total number of packets received by the phone
Rcvr Octets	Total number of octets received by the phone
Rcvr Start Time	Internal time stamp indicating when Cisco Unified Communications Manager requested that the phone start receiving packets
<b>Voice Quality Metrics</b>	
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 the <a href="#">“Monitoring the Voice Quality of Calls” section on page 8-15.</a> <b>Note</b> 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.

**Table 7-6 Streaming Statistics Area Items (continued)**

<b>Item</b>	<b>Description</b>
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: <ul style="list-style-type: none"> <li>• G.711 gives 4.5</li> <li>• G.729 A /AB gives 3.7</li> </ul>
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.





## CHAPTER 8

# Troubleshooting and Maintenance

---

This chapter provides information that can assist you in troubleshooting problems with your Cisco Unified IP Phone or in your IP telephony network.

For additional troubleshooting information, refer to the *Using the 79xx Status Information For Troubleshooting* tech note. This document is available to registered Cisco.com users at this URL:

[http://www.cisco.com/warp/customer/788/AVVID/telecaster\\_trouble.html](http://www.cisco.com/warp/customer/788/AVVID/telecaster_trouble.html)

If you need additional troubleshooting assistance, you can contact the Cisco TAC. The phone generates detailed logs that can assist the Cisco TAC with troubleshooting and resolving problems.

This chapter includes these topics:

- [Resolving Startup Problems, page 8-1](#)
- [Cisco Unified IP Phone Resets Unexpectedly, page 8-6](#)
- [Troubleshooting Cisco Unified IP Phone Security, page 8-9](#)
- [General Troubleshooting Tips, page 8-10](#)
- [General Troubleshooting Tips for the Cisco Unified IP Phone Expansion Module 7914, page 8-12](#)
- [Resetting or Restoring the Cisco Unified IP Phone, page 8-13](#)
- [Using the Quality Report Tool, page 8-15](#)
- [Monitoring the Voice Quality of Calls, page 8-15](#)
- [Where to Go for More Troubleshooting Information, page 8-17](#)
- [Cleaning the Cisco Unified IP Phone, page 8-17](#)

## Resolving 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 “[Verifying the Phone Startup Process](#)” section on [page 3-9](#). If the phone does not start up properly, see the following sections for troubleshooting information:

- [Symptom: The Cisco Unified IP Phone Does Not Go Through its Normal Startup Process, page 8-2](#)
- [Symptom: The Cisco Unified IP Phone Does Not Register with Cisco Unified Communications Manager, page 8-2](#)
- [Symptom: Cisco Unified IP Phone Unable to Obtain IP Address, page 8-6](#)

## Symptom: The Cisco Unified IP Phone Does Not Go Through its Normal Startup Process

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. 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.

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 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:
  - 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.

If after attempting these solutions, the LCD screen on the Cisco Unified IP Phone does not display any characters after at least five minutes, perform a factory reset of the phone (see the [“Performing a Factory Reset”](#) section on page 8-14). If the phone still does not display characters, contact a Cisco technical support representative for additional assistance.

## Symptom: The 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:

- [Identifying Error Messages, page 8-3](#)
- [Registering the Phone with Cisco Unified Communications Manager, page 8-3](#)
- [Checking Network Connectivity, page 8-3](#)
- [Verifying TFTP Server Settings, page 8-3](#)
- [Verifying IP Addressing and Routing, page 8-4](#)
- [Verifying DNS Settings, page 8-4](#)
- [Verifying Cisco Unified Communications Manager Settings, page 8-4](#)

- [Cisco Unified Communications Manager and TFTP Services Are Not Running](#), page 8-4
- [Creating a New Configuration File](#), page 8-5

In addition, problems with security may prevent the phone from starting up properly. See the [“Troubleshooting Cisco Unified IP Phone Security”](#) section on page 8-9 for more information.

## Identifying Error Messages

As the Cisco Unified IP Phones 7960G/7940G cycle through the startup process, you can access status messages that might provide you with information about the cause of a problem. See the [“Status Messages Screen”](#) section on page 6-3 for instructions about accessing status messages and for a list of potential errors, their explanations, and their solutions.

## Registering the Phone with Cisco Unified Communications Manager

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 auto-registration is enabled. Review the information and procedures in the [“Adding Phones to the Cisco Unified Communications Manager Database”](#) section on page 2-7 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 the [“Determining the MAC Address for a Cisco Unified IP Phone”](#) section on page 2-12.

If the phone is already in the Cisco Unified Communications Manager database, its configuration file may be damaged. See the [“Creating a New Configuration File”](#) section on page 8-5 for assistance.

## Checking Network Connectivity

If the network is down between the phone and the TFTP server or Cisco Unified Communications Manager, the phone cannot start up properly. Ensure that the network is currently running.

## Verifying TFTP Server Settings

The Cisco Unified IP Phone uses the TFTP Server 1 setting to identify the primary TFTP server used by the phone. You can determine this setting by pressing the **Settings** button on the phone, choosing **Network Configuration**, and scrolling to the **TFTP Server 1** option.

If you have assigned a static IP address to the phone, you must manually enter a setting for the TFTP Server 1 option. See the [“Network Configuration Menu”](#) section on page 4-4.

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.

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 a from one location to another. See the [“Network Configuration Menu”](#) section on page 4-4 for instructions.

## Verifying IP Addressing and Routing

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.

On the Cisco Unified IP Phone, press the **Settings** button, choose **Network Configuration**, and look at the following options:

- **DHCP Server**—If you have assigned a static IP address to the phone, you do not need to enter a value for the DHCP Server option. However, if you are using a DHCP server, this option must have a value. If it does not, check your IP routing and VLAN configuration. Refer to *Troubleshooting Switch Port Problems*, available at this URL: <http://www.cisco.com/warp/customer/473/53.shtml>
- **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 the “**Network Configuration Menu**” section on page 4-4 for instructions.

If you are using DHCP, check the IP addresses distributed by your DHCP server. Refer to *Understanding and Troubleshooting DHCP in Catalyst Switch or Enterprise Networks*, available at this URL: <http://www.cisco.com/warp/customer/473/100.html#41>

## Verifying DNS Settings

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. Verify this setting by pressing the **Settings** button on the phone, choosing **Network Configuration**, and scrolling to the **DNS Server 1** option. 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.

You must also ensure that DNS is configured to do reverse look-ups.

## Verifying Cisco Unified Communications Manager Settings

On the Cisco Unified IP Phone, press the **Settings** button, choose **Network Configuration**, and look at the **Communications Manager 1–5** options. The Cisco Unified IP Phone attempts to open a TCP connection to all the Cisco Unified Communications Manager servers that are part of the assigned Cisco Unified Communications Manager group. If none of these options contain IP addresses or show Active or Standby, the phone is not properly registered with Cisco Unified Communications Manager. See the “**Registering the Phone with Cisco Unified Communications Manager**” section on page 8-3 for tips on resolving this problem.

## Cisco Unified Communications Manager and TFTP Services Are Not Running

If the Cisco Unified Communications Manager or TFTP services are not running, phones may not be able to start up properly. However, in such a situation, it is likely that you are experiencing a system-wide failure and that other phones and devices are unable to start up properly.

If the Cisco Communications Manager service is not running, all devices on the network that rely on it to make phone calls will be affected. If the TFTP service is not running, many devices will not be able to start up successfully.



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 its radio button and then click the **Start** button. The Service Status symbol changes from a square to an arrow.
- 



#### Note

A service must be activated before it can be started or stopped. To activate a service, choose **Tools > Service Activation**.

---

## Creating a New Configuration File

If you continue to have problems with a particular phone that other suggestions in this chapter do not resolve, the configuration file may be corrupted.

To create a new configuration file, follow these steps:

#### Procedure

- 
- Step 1** From Cisco Unified Communications Manager, choose **Device > Phone > Find** to locate the phone experiencing problems.
- Step 2** Choose **Delete** to remove the phone from the Cisco Unified Communications Manager database.
- Step 3** Add the phone back to the Cisco Unified Communications Manager database. See the [“Adding Phones to the Cisco Unified Communications Manager Database”](#) section on page 2-7 for details.
- Step 4** Power cycle the phone:
- If the phone receives power from an external power source, unplug the Ethernet cable from the Network port on the phone, then unplug the power supply from the DC adaptor port on the phone. Next, reconnect the power supply and then reconnect the Ethernet cable.



#### Caution

Always unplug the upstream Ethernet cable from the phone before unplugging the power supply. Unplugging the power supply before unplugging the upstream Ethernet cable could result in a service interruption on the network.

---

- If the phone receives inline power, unplug the cable from the Network port on the phone and then plug it back in.
-

**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's 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. Refer to Cisco Unified Communications Manager Administration Guide for more information.
- Changing the buttons on a phone button template, or assigning a different phone button template to a phone, may result in directory numbers that are no longer accessible from the phone. The directory numbers are still assigned to the phone in the Cisco Unified Communications Manager database, but 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.

## Symptom: Cisco Unified IP Phone Unable to Obtain IP Address

If a phone is unable to obtain an IP address when it starts up, the phone may not be on the same network or VLAN as the DHCP server, or the switch port to which the phone is connected may be disabled.

Make sure that the network or VLAN to which the phone is connected has access to the DHCP server, and make sure that the switch port is enabled.

## 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:

- [Verifying Physical Connection, page 8-6](#)
- [Identifying Intermittent Network Outages, page 8-7](#)
- [Verifying DHCP Settings, page 8-7](#)
- [Checking Static IP Address Settings, page 8-7](#)
- [Verifying Voice VLAN Configuration, page 8-7](#)
- [Verifying that the Phones Have Not Been Intentionally Reset, page 8-8](#)
- [Eliminating DNS or Other Connectivity Errors, page 8-8](#)

## Verifying Physical Connection

Verify that the Ethernet connection to which the Cisco Unified IP Phone is connected is up. For example, check if the particular port or switch to which the phone is connected is down.

## Identifying Intermittent Network Outages

Intermittent network outages affect data and voice traffic differently. Your network might have been 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 its network connection.

If you are experiencing problems with the voice network, you should investigate whether an existing problem is simply being exposed.

## Verifying DHCP Settings

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 the [“Network Configuration Menu” section on page 4-4](#) 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 it 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 will be denied, forcing the phone to restart and request a new IP address from the DHCP server.

## Checking Static IP Address Settings

If the phone has been assigned a static IP address, verify that you have entered the correct settings. See the [“Network Configuration Menu” section on page 4-4](#) for more information.

## Verifying Voice VLAN Configuration

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.

Isolating the phones on a separate auxiliary VLAN increases the quality of the voice traffic. See the [“Understanding How the Cisco Unified IP Phone Interacts with the VLAN” section on page 2-3](#) for details.

## Verifying that the Phones Have Not Been Intentionally Reset

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.

You can check whether a Cisco Unified IP Phone 7960G/7940G received a command from Cisco Unified Communications Manager to reset by pressing the **Settings** button on the phone and choosing **Status > Network Statistics**. If the phone was recently reset one of these messages appears:

- Reset-Reset—Phone closed due to receiving a Reset/Reset from Cisco Unified Communications Manager administration.
- Reset-Restart—Phone closed due to receiving a Reset/Restart from Cisco Unified Communications Manager administration.

## Eliminating DNS or Other Connectivity Errors

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

### Procedure

- 
- Step 1** Reset the phone to factory defaults. See the [“Resolving Startup Problems” section on page 8-1](#) for details.
- Step 2** Modify DHCP and IP settings:
- Disable DHCP. See the [“Network Configuration Menu” section on page 4-4](#) for instructions.
  - Assign static IP values to the phone. See the [“Network Configuration Menu” section on page 4-4](#) for instructions. Use the same default router setting used for other functioning Cisco Unified IP Phones.
  - Assign a TFTP server. See the [“Network Configuration Menu” section on page 4-4](#) for instructions. Use the same TFTP server used for other functioning Cisco Unified IP Phones.
- Step 3** On the Cisco Unified Communications Manager server, verify that the local host files have the correct Cisco Unified Communications Manager server name mapped to the correct IP address.
- Step 4** From Cisco Unified Communications Manager, choose **System > Server** and verify that the server is referred to by 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 the [“Determining the MAC Address for a Cisco Unified IP Phone” section on page 2-12](#).
- Step 6** Power cycle the phone:
- If the phone receives power from an external power source, unplug the Ethernet cable from the Network port on the phone, then unplug the power supply from the DC adaptor port on the phone. Next, reconnect the power supply and then reconnect the Ethernet cable.



### Caution

Always unplug the upstream Ethernet cable from the phone before unplugging the power supply. Unplugging the power supply before unplugging the upstream Ethernet cable could result in a service interruption on the network.

- If the phone receives inline power, unplug the cable from the Network port on the phone and then plug it back in.

# Troubleshooting Cisco Unified IP Phone Security

Table 8-1 provides troubleshooting information for the security features on the Cisco Unified IP Phone. For information relating to the solutions for any of these issues, and for additional troubleshooting information about security and encryption, refer to *Cisco Unified Communications Manager Security Guide*.

Because third-party troubleshooting tools that sniff media and TCP packets do not work after you enable encryption, you must use Cisco Unified Communications Manager Administration to perform the following tasks if a problem occurs:

- Analyze TCP packets for SCCP messages that are exchanged between Cisco Unified Communications Manager and the device
- Extract the media encryption key material from SCCP messages and decrypt the media between the devices

**Table 8-1** Cisco Unified IP Phone Security Troubleshooting

Problem	Possible Cause
LSC fails on the phone.	CAPF configuration error.
Device authentication error.	CTL file does not have a Cisco Unified Communications Manager certificate or has an incorrect certificate.
Phone cannot authenticate CTL file.	The security token that signed the updated CTL file does not exist in the CTL file on the phone.
Phone cannot authenticate any of the configuration files other than the CTL file.	Bad TFTP record.
Phone reports TFTP authorization failure.	<ul style="list-style-type: none"> <li>• The TFTP address for the phone does not exist in the CTL file.</li> <li>• If you created a new CTL file with a new TFTP record, the existing CTL file on the phone may not contain a record for the new TFTP server.</li> </ul>
Phone does not register with Cisco Unified Communications Manager.	The CTL file does not contain the correct information for the Cisco Unified Communications Manager server.
Phone does not interact with the correct CAPF server to obtain the locally-significant certificate.	<ul style="list-style-type: none"> <li>• The CAPF utility runs on a different workstation/server than is specified in the CTL file.</li> <li>• The CAPF certificate has changed since the last update of the CTL file.</li> </ul>
Phone does not request signed configuration files.	<ul style="list-style-type: none"> <li>• The CTL file does not contain any TFTP server entry.</li> <li>• The CTL file does not contain any TFTP entries with certificates</li> </ul>

# General Troubleshooting Tips

Table 8-2 provides general troubleshooting information for the Cisco Unified IP Phone.

**Table 8-2** Cisco Unified IP Phone Troubleshooting


Summary	Explanation
Connecting a Cisco Unified IP Phone to another Cisco Unified IP Phone/	Cisco does not support connecting an IP phone to another IP phone through the PC port. Each IP phone should directly connect to a switch port. If phones are connected together in a line (by using the PC port), the phones will not work.
Poor quality when calling digital mobile phones using the G.729 protocol.	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 mobile phone will have poor voice quality. Use G.729 only when absolutely necessary.
Prolonged broadcast storms cause IP phones to re-register.	Prolonged broadcast storms (lasting several minutes) on the voice VLAN cause the IP phones to re-register with another Cisco Unified Communications Manager server.
Moving a network connection from the phone to a workstation.	<p>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.</p> <p> <b>Caution</b> The computer's network card cannot receive power through the network connection; if power comes through the connection, the network card can be destroyed. To protect a network card, wait 10 seconds or longer after unplugging the cable from the phone before plugging it into a computer. This delay gives the switch enough time to recognize that there is no longer a phone on the line and to stop providing power to the cable.</p>
Changing the telephone configuration.	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 the <a href="#">“Unlocking and Locking Options”</a> section on page 4-2 for details.
Phone resetting.	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.
LCD display issues.	If the display appears to have rolling lines or a wavy pattern, it might be interacting with certain types of older fluorescent lights in the building. Moving the phone away from the lights, or replacing the lights, should resolve the problem.
Dual-Tone Multi-Frequency (DTMF) delay.	When you are on a call that requires keypad input, if you press the keys too quickly, some of them might not be recognized.
Codec mismatch between the phone and another device.	<p>The RxType and the TxType statistics show the codec that is being used for a conversation between this IP phone and the other device. The values of these statistics should match. If they do not, verify that the other device can handle the codec conversation or that a transcoder is in place to handle the service.</p> <p>See the <a href="#">“Call Statistics Screen”</a> section on page 6-10 for information about displaying these statistics.</p>

Table 8-2 Cisco Unified IP Phone Troubleshooting (continued)

Summary	Explanation
Sound sample mismatch between the phone and another device.	<p>The RxSize and the TxSize statistics show the size of the voice packets that are being used in a conversation between this IP phone and the other device. The values of these statistics should match.</p> <p>See the “<a href="#">Call Statistics Screen</a>” section on page 6-10 for information about displaying these statistics.</p>
Gaps in voice calls.	<p>Check the AvgJtr and the MaxJtr statistics. A large variance between these statistics might indicate a problem with jitter on the network or periodic high rates of network activity.</p> <p>See the “<a href="#">Call Statistics Screen</a>” section on page 6-10 for information about displaying these statistics.</p>
Checking signaling.	To check that signaling is working properly between the phone and Cisco Unified Communications Manager, press the <b>Speaker</b> button on the phone to answer a call. If you can answer a call and if you hear a dial tone, signaling is working properly.
Checking the handset cradle clip.	<p>Cisco Unified IP Phones are designed with a reversible handset clip in the cradle. This clip is used with the plastic tab protruding out when the phone is in a vertical (wall-mounted) position. The position of the tab can interfere with the handset as it is placed in the cradle. If the phone remains in the on-hook position you may experience continued ringing when you try to answer a call or a lack of dial tone when you try to place a call. To resolve this problem, you may need to reverse the clip.</p> <p>If the handset cradle clip is in the wall-mounted position and your phone is placed on a desktop, slide the clip upward to remove it. Rotate the clip 180 degrees and slide it back in so that the tab is hidden.</p> <p>If the hook switch remains in the down position, tapping on the phone should free up the switch. You can also try pushing and suddenly releasing the off-hook button after the handset has been picked up.</p>
Checking the hook switch contacts.	The hook switch contacts on the phone use a wiping action to self-clean the contacts. If your phone is not used regularly, dust and other airborne contaminants may degrade the contact performance and cause problems with operation. If you have periods of limited phone usage, you can clean the contacts by quickly pressing and releasing the hook switch a dozen times.
Checking the position of the phone.	The footstand of the phone allows adjustment of the phone to eliminate glare on the LCD screen. When the phone is in the most vertical position, the phone may be forced forward and the handset may not sit properly in the cradle, creating a false off-hook condition. Cisco recommends that you position the phone one notch from the most vertical position to ensure that the handset is firmly resting on the hook switch.
Checking the LAN cable.	Make sure that the LAN cable connected to the phone is positioned properly. The LAN cable should pass out of the side of the phone between the base and the footstand. If you are using a cable (such as Cat-5E or Cat-6) with a larger diameter than the cable that was packaged with your phone, the cable may cause the phone to tilt forward and force it off-hook. Use a smaller LAN cable to eliminate this problem.

**Table 8-2** Cisco Unified IP Phone Troubleshooting (continued)

Summary	Explanation
Loopback condition.	<p>A loopback condition can occur when the following conditions are met:</p> <ul style="list-style-type: none"> <li>• The SW Port Configuration option in the Network Configuration menu on the phone is set to <b>10H</b> (10-BaseT / half duplex)</li> <li>• The phone receives power from an external power supply.</li> <li>• The phone is powered down (the power supply is disconnected).</li> </ul> <p>In this case, the switch port on the phone can become disabled and the following message will appear in the switch console log:</p> <pre>HALF_DUX_COLLISION_EXCEED_THRESHOLD</pre> <p>To resolve this problem, re-enable the port from the switch.</p>

## General Troubleshooting Tips for the Cisco Unified IP Phone Expansion Module 7914

[Table 8-3](#) provides general troubleshooting information for the Cisco Unified IP Phone Expansion Module 7914.

**Table 8-3** Cisco Unified IP Phone Expansion Module 7914 Troubleshooting

Problem	Solution
No display on the Cisco Unified IP Phone Expansion Module 7914	<p>Verify that all of the cable connections are correct.</p> <p>Verify that you have power to the Cisco Unified IP Phone Expansion Module 7914.</p>
Lighted buttons on the first Cisco Unified IP Phone Expansion Module 7914 are all red.	Verify that the Cisco Unified IP Phone Expansion Module 7914 is defined in Cisco Unified Communications Manager.
Lighted buttons on the second Cisco Unified IP Phone Expansion Module 7914 are all amber.	Verify that the Cisco Unified IP Phone Expansion Module 7914 is defined in Cisco Unified Communications Manager.



# Resetting or Restoring the Cisco Unified IP Phone

There are two general methods for resetting or restoring the Cisco Unified IP Phone:

- [Performing a Basic Reset, page 8-13](#)
- [Performing a Factory Reset, page 8-14](#)

## Performing a 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.

There are several ways to perform a basic reset, as described in [Table 8-4](#). You can reset a phone with any of these operations after the phone has started up. Choose the operation that is appropriate for your situation.



### Note

You can use the Erase Configuration option in the Network Configuration menu to change these settings to their default values: Network Configuration menu settings (including password), Device Configuration menu settings, volume settings, and contrast settings. To use this feature, choose **Settings > Network Configuration**, scroll to the Erase Configuration option, press the **Yes** softkey, then press the **Save** softkey.

**Table 8-4** Basic Reset Methods

Operation	Performing	Explanation
Restore configuration changes and restart phone	From the Settings screen, press <b>****</b> .	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.
<b>Restore</b> softkey	Choose <b>Settings &gt; more</b> and then press the <b>Restore</b> softkey.	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.
<b>Default</b> softkey	Choose <b>Settings &gt; more</b> and press the <b>Default</b> softkey.	Resets ring type, display contrast, handset volume, headset volume, speaker volume, and ringer volume to their default values.
<b>Erase</b> softkey	Unlock phone options (see the <a href="#">“Unlocking and Locking Options”</a> section on page 4-2). Then choose <b>Settings &gt; more</b> and press the <b>Erase</b> softkey.	Resets user and network configuration settings to their default values, deletes the CTL file from the phone, and restarts the phone.

## Performing a Factory Reset

When you perform a factory reset of the Cisco Unified IP Phone, the following information is erased or reset to its default value:

- CTL file—Erased
- LSC—Erased
- User configuration settings—Reset to default values
- Network configuration settings—Reset to default values (optional)
- Locale information—Reset to default value
- Call histories—Erased

To perform a factory reset of a phone, perform the following steps.



### Note

If the phone is not in a DHCP-enabled network, it will not automatically discover its network configuration and register with Cisco Unified Communications Manager after it resets. In this case, you must configure the phone manually after it resets.

### Procedure

- 
- Step 1** Unplug the power cable from the phone and then plug it back in.  
The phone begins its power up cycle.
- Step 2** Immediately press and hold # while the Headset, Mute, and Speaker buttons turn on and off in sequence. Release # after the Speaker button turns off.  
The Headset, Mute, and Speaker buttons flash in sequence to indicate that the phone is waiting for you to enter the key sequence for the reset.
- Step 3** Press **123456789\*0#** within 60 seconds after the Headset, Mute, and Speaker buttons begin to flash.  
If you repeat a key within the sequence (for example, if you press **1223456789\*0#**), the sequence will still be accepted and the phone will reset.  
If you do not complete this key sequence or do not press any keys, the Headset, Mute, and Speaker buttons will stop flashing after 60 seconds and the phone will continue with its normal startup process. The phone will not reset.  
If you enter an invalid key sequence, the buttons will stop flashing immediately and the phone will continue with its normal startup process. The phone will not reset.  
If you enter this key sequence correctly, the phone displays this prompt:  
`Keep network cfg? 1 = yes 2 = no`
- Step 4** To maintain existing network configuration settings for the phone when the phone resets, press **1**. To reset network configuration settings when the phone resets, press **2**.  
If you press another key or do not respond to this prompt within 60 seconds, the will continue with its normal startup process and will not reset.  
Otherwise, the phone goes through the factory reset process.
-

## Using the Quality Report Tool

The Quality Report Tool (QRT) is a voice quality and general problem-reporting tool for the Cisco Unified IP Phone 7960G/7940G. This tool is installed as part of the Cisco Unified Communications Manager installation.

You can configure users' Cisco Unified IP Phone with QRT so they can report problems with phone calls. Users can report issues by using the Cisco Unified IP Phone softkey labeled QRT. The QRT softkey is available only when the Cisco Unified IP Phone is in the Connected, Connected Conference, Connected Transfer, and/or OnHook states.

When users press the **QRT** softkey on their IP phone, they are presented with a list of problem categories. Users can then choose the appropriate problem category, and their feedback is logged in an XML file. Actual information logged depends on the user selection and whether the destination device is a Cisco Unified IP Phone.

For more information about using QRT, refer to *Cisco Unified Communications Manager Features and Services Guide*.

## Monitoring the Voice Quality of Calls

To measure the voice quality of calls that are sent and received within the network, Cisco Unified IP Phones use these statistical metrics that are based on concealment events. The DSP plays concealment frames to mask frame loss in the voice packet stream.

- Concealment Ratio metrics—Show the ratio of concealment frames over total speech frames. An interval conceal ratio is calculated every 3 seconds.
- Concealed Second metrics—Show the number of seconds in which the DSP plays concealment frames due to lost frames. A severely “concealed second” is a second in which the DSP plays more than five percent concealment frames.
- MOS-LQK metrics—Use a numeric score to estimate the relative voice listening quality. The Cisco Unified IP Phone calculates the mean opinion score (MOS) for listening quality (LQK) based on audible concealment events due to frame loss in the preceding 8 seconds, and includes perceptual weighting factors such as codec type and frame size.

MOS LQK scores are produced by a Cisco proprietary algorithm that is an implementation of P.VTQ, an ITU provisional standard.



### 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.

For information about configuring voice quality metrics for phones, refer to the “Phone Features” section in the “Cisco Unified IP Phone” chapter in *Cisco Unified Communications Manager System Guide*.

You can access voice quality metrics from the Cisco Unified IP Phone by using the Call Statistics screen (see the [“Call Statistics Screen”](#) section on page 6-10) or remotely by using Streaming Statistics (see [Chapter 7, “Monitoring the Cisco Unified IP Phone Remotely”](#)).

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.719A/ AB gives 3.7 score

A Conceal Ratio of zero indicates that the IP network is delivering frames and packets on time with no loss.

When you observe significant and persistent changes to metrics, use [Table 8-5](#) for general troubleshooting information:

**Table 8-5** Changes to Voice Quality Metrics

Metric Change	Condition
MOS LQK scores decrease significantly	<p>Network impairment from packet loss or high jitter:</p> <ul style="list-style-type: none"> <li>• Average MOS LQK decreases could indicate widespread and uniform impairment.</li> <li>• Individual MOS LQK decreases indicate bursty impairment.</li> </ul> <p>Cross-check with Conceal Ratio and Conceal Seconds for evidence of packet loss and jitter.</p>
MOS LQK scores decrease significantly	<ul style="list-style-type: none"> <li>• Check to see if the phone is using a different codec than expected (RxType and TxType).</li> <li>• Check to see if the MOS LQK version changed after a firmware upgrade.</li> </ul>
Conceal Ratio and Conceal Seconds increase significantly	<ul style="list-style-type: none"> <li>• Network impairment from packet loss or high jitter.</li> </ul>
Conceal Ratio is near or at zero, but the voice quality is poor	<ul style="list-style-type: none"> <li>• Noise or distortion in the audio channel such as echo or audio levels.</li> <li>• Tandem calls that undergo multiple encode/decode such as calls to a mobile network or calling card network.</li> <li>• Acoustic problems coming from a speakerphone, handsfree mobile phone or wireless headset.</li> </ul> <p>Check packet transmit (TxCnt) and packet receive (RxCnt) counters to verify that voice packets are flowing.</p>

Voice quality metrics do not account for noise or distortion, only frame loss.

## Where to Go for More Troubleshooting Information

If you have additional questions about troubleshooting the Cisco Unified IP Phones, several Cisco.com web sites can provide you with more tips. Choose from the sites available for your access level.

- Cisco Unified IP Phone Troubleshooting Resources:  
[http://www.cisco.com/en/US/products/hw/phones/ps379/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/hw/phones/ps379/tsd_products_support_series_home.html)
- Cisco Products and Services (Technical Support and Documentation):  
<http://www.cisco.com/web/psa/products/index.html>

## Cleaning the Cisco Unified IP Phone

To clean your Cisco Unified IP phone, use only a dry soft cloth to gently wipe the phone and the LCD 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.





## APPENDIX **A**

# Providing Information to Users Via a Website

---

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.

Consider including the following types of information on this site:

- [How Users Obtain Support for the Cisco Unified IP Phone, page A-1](#)
- [Giving Users Access to the User Options Web Pages, page A-1](#)
- [How Users Get Copies of Cisco Unified IP Phone Manuals, page A-2](#)
- [Accessing Cisco 7900 Series Unified IP Phone eLearning Tutorials, page A-2](#)
- [How Users Subscribe to Services and Configure Phone Features, page A-2](#)
- [How Users Access a Voice Messaging System, page A-3](#)
- [How Users Configure Personal Directory Entries, page A-3](#)

## How Users Obtain Support for the Cisco Unified IP Phone

To successfully use some of the features on the Cisco Unified IP Phone (including speed dial, services, and voice messaging system options), users must receive information from you or from your network team or be able to contact you for assistance. Make sure to provide end users with the names of people to contact for assistance and with instructions for contacting those people.

## Giving Users Access to the User Options Web Pages

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 additional information, refer to:

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

## How Users Get Copies of Cisco Unified IP Phone Manuals

You should provide end users with access to user documentation for the Cisco Unified IP Phones. *Cisco Unified IP Phone 7960G and 7940G Phone 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 end users on your website.

For a list of available documentation for Cisco Unified IP Phones, go to this URL:

[http://www.cisco.com/en/US/products/hw/phones/ps379/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/hw/phones/ps379/tsd_products_support_series_home.html)

For a list of available documentation for Cisco Unified Communications Manager, go to this URL:

[http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html)

For more information about viewing or ordering documentation, see the “Obtaining Documentation, Obtaining Support, and Security Guidelines” section on page xiii.

## Accessing Cisco 7900 Series Unified IP Phone eLearning Tutorials

Cisco 7900 Series Unified IP Phone 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 7961G/G-GE, 7941G/G-GE, 7960G, 7940G, 7912G, and 7905G.

End-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:

[http://cisco.com/en/US/products/hw/phones/ps379/products\\_user\\_guide\\_list.html](http://cisco.com/en/US/products/hw/phones/ps379/products_user_guide_list.html)

Administrators can download customizable versions of the eLearning tutorials (English only) from the phone product pages on cisco.com at

[http://cisco.com/en/US/products/hw/phones/ps379/prod\\_models\\_home.html](http://cisco.com/en/US/products/hw/phones/ps379/prod_models_home.html)

Refer to the tutorial Read Me file included with the relevant eLearning tutorial for specific instructions, including how to link to the most recent user guide PDF.



### Note

The eLearning tutorials are updated periodically and therefore might not contain the latest feature information for end-users. For the latest feature information, end-users should refer to the Cisco Unified IP Phone end-user documentation specific to their phone model and Cisco Unified Communications Manager version.

## How Users Subscribe to Services and Configure Phone Features

End users can perform a variety of activities by using the Cisco Unified Communications Manager User Options web pages. These activities include subscribing to services, setting up speed dial and call forwarding numbers, configuring ring settings, and creating a personal address book. Keep in mind that



configuring settings on a phone by using a website might be new for your end 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 end users with the following information about the User Options web pages:

- The URL required to access the application. This URL is:  
`http://server_name:portnumber/ccmuser/`, where *server\_name* is the host on which the web server is installed.
- A user ID and default password are needed to access the application.  
These settings correspond to the values you entered when you added the user to Cisco Unified Communications Manager (see the [“Adding Users to Cisco Unified Communications Manager” section on page 5-17](#)).
- A brief description of what a web-based, graphical user interface application is, and how to access it with a web browser.
- An overview of the tasks that users can accomplish by using the web page.

## How Users Access a Voice Messaging System

Cisco Unified Communications Manager lets you integrate with many 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.

## How Users Configure Personal Directory Entries

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 the [“How Users Subscribe to Services and Configure Phone Features” section on page A-2](#) for details.
- Cisco Unified IP Phone Address Book Synchronizer—Make sure to provide users with the installer for this application. To obtain the installer, choose **Application > Plugins** from Cisco Unified Communications Manager Administration and click **Download**, which is located next to the **Cisco Unified IP Phone Address Book Synchronizer** plugin name. When the file download dialog box displays, click **Save**. Send the TabSyncInstall.exe file to all users who require this application.

See the [“Installing and Configuring the Cisco Unified IP Phone Address Book Synchronizer”](#) section on page A-4 for information about installing the Cisco Unified IP Phone Address Book Synchronizer.

## Installing and Configuring the Cisco Unified IP Phone Address Book Synchronizer

Use this tool to synchronize data stored in your Microsoft Windows address book with the Cisco Unified Communications Manager directory and the User Options Personal Address Book.



### Tip

To successfully synchronize the Windows address book with the Personal Address Book, all Windows address book users should be entered in the Windows address book before performing the following procedures.

### Installing the Synchronizer

- 
- Step 1** Get the Cisco Unified IP Phone Address Book Synchronizer installer file from your system administrator.
  - Step 2** Double-click the TabSyncInstall.exe file provided by your system administrator.  
The publisher dialog box displays.
  - Step 3** Click **Run**.  
The Welcome to the InstallShield Wizard for Cisco Unified CallManager Personal Address Book Synchronizer window displays.
  - Step 4** Click **Next**.  
The License Agreement window displays.
  - Step 5** Read the license agreement information, and click the I Accept radio button. Click **Next**.  
The Destination Location window displays.
  - Step 6** Choose the directory in which you want to install the application and click **Next**.  
The Ready to Install window displays.
  - Step 7** Click **Install**.  
The installation wizard installs the application to your computer. When the installation is complete, the InstallShield Wizard Complete window displays.
  - Step 8** Click **Finish**.
  - Step 9** To complete the process, follow the steps in the [“Configuring the Synchronizer”](#) section on page A-4.
- 

### Configuring the Synchronizer

- 
- Step 1** Open the Cisco Unified IP Phone Address Book Synchronizer.  
If you accepted the default installation directory, you can open the application by choosing **Start > All Programs > Cisco Systems > TabSync**.
  - Step 2** To configure user information, click the **User** button.

The Cisco Unified CallManager User Information window displays.

**Step 3** Enter the Cisco Unified IP Phone user name and password and click **OK**.

**Step 4** To configure Cisco Unified Communications Manager server information, click the **Server** button.

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 click **OK**.

If you do not have this information, contact your system administrator.

**Step 6** To start the directory synchronization process, click the **Synchronize** button.

The Synchronization Status window provides information on 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. Choose the entry that you want to include in your Personal Address Book and click **OK**.

When synchronization completes, click **Exit** to close the Cisco Unified CallManager Address Book Synchronizer. To verify if the synchronization worked, log in to your User Options web pages and choose Personal Address Book. The users from your Windows address book should be listed.

---





# APPENDIX **B**

## Feature Support by Protocol for Cisco Unified IP Phone 7960G and 7940G

This appendix provides information about feature support for the Cisco Unified IP Phone 7960G and 7940G using the SCCP or SIP protocol with Cisco Unified Communications Manager Release 7.0.

[Table B-1](#) 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 7960G and 7940G Phone Guide for Cisco Unified Communications Manager 7.0*.

This guide is available at this URL:

[http://www.cisco.com/en/US/products/hw/phones/ps379/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/hw/phones/ps379/tsd_products_support_series_home.html)

The specific sections that describe the features in the phone guide are referenced in [Table B-1](#).

**Table B-1** Cisco Unified IP Phone 7960G and 7940G Feature Support by Protocol

Features	Cisco Unified IP Phones 7960G, 7940G		For More Information
	SCCP	SIP	
<b>Calling Features</b>			
Abbreviated Dialing	Supported	Not supported	“Basic Call Handling—Placing a Call: Additional Options”
Auto Answer	Supported	Supported	“Using a Handset, Headset, and Speakerphone—Using Auto Answer”
Barge (and cBarge)	Supported	Not supported	“Advanced Call Handling—Using a Shared Line”
Busy Lamp Field (BLF) speed dial	Supported	Supported	“Advanced Call Handling—Using BLF to Determine a Line State”
Call Back	Supported	Not supported	“Basic Call Handling—Placing a Call: Additional Options”
Call Display Restrictions	Supported	Supported	“Basic Call Handling—Forwarding Calls to Another Number”
Call Forward All	Supported	Supported	“Basic Call Handling—Forwarding Calls to Another Number”
Call Forward Busy	Supported	Supported	“Basic Call Handling—Forwarding Calls to Another Number”

Table B-1 Cisco Unified IP Phone 7960G and 7940G Feature Support by Protocol (continued)

Features	Cisco Unified IP Phones 7960G, 7940G		For More Information
	SCCP	SIP	
<b>Calling Features</b>			
Call Forward No Answer	Supported	Supported	“Basic Call Handling—Forwarding Calls to Another Number”
Call Park	Supported	Not supported	“Advanced Call Handling—Storing and Receiving Parked Calls”
Call Pickup	Supported	Not supported	“Advanced Call Handling—Picking Up a Redirected Call on Your Phone”
Call Waiting	Supported	Supported	“Basic Call Handling—Answering a Call”
Caller ID	Supported	Supported	“An Overview of Your Phone—Understanding Touch Screen Features” or “An Overview of Your Phone—Understanding Phone Screen Features”
Conference	Supported	Supported	“Basic Call Handling—Making Conference Calls”
Do Not Disturb (DND)	Supported	Not supported	“Basic Call Handling—Using Do Not Disturb”
Extension Mobility	Supported	Not supported	“Advanced Call Handling—Using Cisco Extension Mobility”
Fast Dial Service	Supported	Supported	“Advanced Call Handling—Speed Dialing”
Hold/Resume	Supported	Supported	“Basic Call Handling—Using Hold and Resume”
Immediate Divert	Supported	Not supported	“Basic Call Handling—Answering a Call”
Join/Select	Supported	Not supported	“Basic Call Handling—Making Conference Calls”
Malicious Call ID	Supported	Supported	“Advanced Call Handling—Tracing Suspicious Calls”
Meet-Me Conference	Supported	Supported	“Basic Call Handling—Making Conference Calls”
Message Waiting Indicator	Supported	Not supported	“Accessing Voice Messages”
Multilevel Precedence and Preemption (MLPP)	Supported	Not supported (SIP)	“Advanced Call Handling—Prioritizing Critical Calls”
Multiple Calls per Line Appearance	200	50	“An Overview of Your Phone—Understanding Lines vs. Calls”
Music on Hold	Supported	Supported	“Basic Call Handling—Using Hold and Resume”
Mute	Supported	Supported	“Basic Call Handling—Using Mute”
On-hook call transfer	Supported	Supported	“Basic Call Handling—Placing a Call: Basic Options”
Other Group Pickup	Supported	Supported	
Privacy	Supported	Not supported	“Advanced Call Handling—Using a Shared Line”
Quality Reporting Tool (QRT)	Supported	Supported	“Troubleshooting—Using the Quality Reporting Tool”
Redial	Supported	Supported	“Basic Call Handling—Placing a Call: Basic Options”
Shared Line	Supported	Not supported	“Advanced Call Handling—Using a Shared Line”

Table B-1 Cisco Unified IP Phone 7960G and 7940G Feature Support by Protocol (continued)

Features	Cisco Unified IP Phones 7960G, 7940G		For More Information
	SCCP	SIP	
<b>Calling Features</b>			
Speed Dialing	Supported	Supported	“Advanced Call Handling—Speed Dialing”
Transfer	Supported	Supported	“Basic Call Handling—Transferring Calls”
Video Support	Supported	Not supported	“Understanding Additional Configuration Options”
Voice Messaging System	Supported	Supported	“Accessing Voice Messages” section of the Phone Guide
<b>Settings</b>			
Call Statistics	Supported	Supported	“Troubleshooting Your Phone—Viewing Phone Administrative Data”
Voice Quality Metrics	Supported	Not supported	“Troubleshooting Your Phone—Viewing Phone Administrative Data”
<b>Services</b>			
SDK Compliance	Supported	Supported	<i>Cisco Unified IP Phone Service Application Development Notes for Release 4.1(3) or later</i>
<b>Directories</b>			
Call Logs	Supported	Supported	“Using Call Logs and Directories—Directory Dialing”
Corporate Directories	Supported	Supported	“Using Call Logs and Directories—Directory Dialing”
Personal Directory Enhancements	Supported	Supported	“Using Call Logs and Directories—Directory Dialing”
<b>Supplemental Features and Applications</b>			
Cisco Unified Communications Manager Assistant	Supported	Supported	<i>Cisco Unified Communications Manager Assistant User Guide</i>
Cisco Unified Communications Manager AutoAttendant	Supported	Supported	<i>Cisco Unified Communications Manager Features and Services Guide</i>
Cisco Unified Communications Manager Attendant Console	Supported	Supported	<i>Cisco Unified Communications Manager Attendant Console User Guide</i>







## Supporting International Users

---

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, refer to the following sections to ensure that the phones are set up properly for your users:

- [Adding Language Overlays to Phone Buttons, page C-1](#)
- [Installing the Cisco Unified Communications Manager Locale Installer, page C-1](#)

### Adding Language Overlays to Phone Buttons

To support the needs of international users, the button labels on the Cisco Unified IP Phones exhibit icons rather than text to indicate the purposes of the buttons. You can purchase language-specific text overlays to add to a phone. To order these language-specific overlays, go to this website:

<http://www.overlaypro.com/cisco/>



**Note**

---

Phone overlays are available only for languages in which the Cisco Unified IP Phone software has been localized. All languages may not be immediately available, so continue to check the website for updates.

---

### Installing the Cisco Unified Communications Manager Locale Installer

If you are using Cisco Unified IP Phones in a locale other than English (United States), you should install the Cisco Unified Communications Manager Locale Installer on every Cisco Unified Communications Manager server in the cluster. Installing the locale installer ensures that you have the latest translated text, user and network locales, and country-specific phone tones available for the Cisco Unified IP Phones. For more information, refer to *Using the Cisco Unified Communications Manager Telephony Locale Installer*.





## Technical Specifications

---

The following sections describe the technical specifications for the Cisco Unified IP Phone 7960G and 7940G.

- [Physical and Operating Environment Specifications, page E-1](#)
- [Cable Specifications, page E-2](#)
- [Network and Access Port Pinouts, page E-2](#)

## Physical and Operating Environment Specifications

[Table E-1](#) shows the physical and operating environment specifications for the Cisco Unified IP Phone 7960G and 7940G.

**Table E-1**      *Physical and Operating Specifications*

Specification	Value or Range
Operating temperature	32° to 104°F (0° to 40°C)
Operating relative humidity	10% to 95% (non-condensing)
Storage temperature	14° to 140°F (–10° to 60°C)
Height	8 in. (20.32 cm)
Width	10.5 in. (26.67 cm)
Depth	6 in. (15.24 cm)
Weight	3.5 lb (1.6 kg)
Power	<ul style="list-style-type: none"><li>• 100-240 VAC, 50-60 Hz, 0.5 A—when using the AC adapter</li><li>• 48 VDC, 0.2 A—when using the in-line power over the network cable</li></ul>
Cables	Two (2) pair of Category 3 for 10-Mbps cables Two (2) pair of Category 5 for 100-Mbps cables
Distance Requirements	As supported by the Ethernet Specification, it is assumed that most Cisco Unified IP Phones should be within 330 feet (100m) of a phone closet.

# Cable Specifications

- RJ-9 jack (4-conductor) for handset and headset connection.
- RJ-11 jack for console access (labeled AUX or RS232).
- RJ-45 jack for the LAN 10/100BaseT connection (labeled LAN).
- RJ-45 jack for a second 10/100BaseT compliant connection (labeled PC).
- 48-volt power connector. The diameter of the center pin in the phone power jack (Switchcraft 712A) is 0.1 in. (2.5 mm). The center pin is positive (+) voltage. The miniature power plug required to mate with the power jack on the phone is a Switchcraft 760 or equivalent.

## 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.

### Network Port Connector

[Table E-2](#) describes the network port connector pinouts.

**Table E-2** Network Port Connector Pinouts

Pin Number	Function
1	TD+
2	TD-
3	RD+
4	+48 Volts return <sup>1</sup>
5	+48 Volts return <sup>1</sup>
6	RD-
7	+48 Volts source <sup>1</sup>
8	+48 Volts source <sup>1</sup>

1. When used to receive power from an inline power card in the Cisco Catalyst switch.

### Access Port Connector

[Table E-3](#) describes the access port connector pinouts.

**Table E-3** Access Port Connector Pinouts

Pin Number	Function
1	RD+
2	RD-
3	TD+
4	Not Used
5	Not Used

**Table E-3** Access Port Connector Pinouts (continued)

Pin Number	Function
6	TD-
7	Not Used
8	Not Used





## APPENDIX **F**

# Basic Phone Administration Steps

---

This appendix provides minimum, basic configuration steps for you to do the following:

- 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.

This section contains these topics:

- [Example User Information for these Procedures, page F-1](#)
- [Adding a User to Cisco Unified Communications Manager, page F-2](#)
- [Configuring the Phone, page F-3](#)
- [Performing Final End User Configuration Steps, page F-8](#)

## Example User Information for these Procedures

In the procedures that follow, example are given when possible to illustrate some of the steps. Sample user and phone information used throughout these procedures includes:

- User's Name: John Doe
- User ID: johndoe
- Phone model: 7961G
- Protocol: SCCP
- MAC address listed on phone: 00127F576611
- Five-digit internal telephone number: 26640

# Adding a User to Cisco Unified Communications Manager

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:

- [Adding a User From an External LDAP Directory, page F-2](#)
- [Adding a User Directly to Cisco Unified Communications Manager, page F-2](#)

## Adding a User From an External LDAP Directory

If you added a user to an LDAP Directory (a non-Cisco Unified Communications Server directory), you can immediately synchronize that directory to the Cisco Unified Communications Manager on which you are adding this same user and the user's phone by following these steps:

### Procedure

---

**Step 1** Log onto Cisco Unified Communications Manager Administration.

**Step 2** Choose **System > LDAP > LDAP Directory**.

**Step 3** Use the **Find** button to locate your LDAP directory.

**Step 4** Click on the LDAP directory name.

**Step 5** Click **Perform Full Sync Now**.




---

**Note** If you do not need to immediately synchronize the LDAP Directory to the Cisco Unified Communications Manager, the LDAP Directory Synchronization Schedule on the LDAP Directory window determines when the next auto-synchronization is scheduled. However, the synchronization must occur before you can associate a new user to a device.

---

**Step 6** Proceed to [Configuring the Phone, page F-3](#)

---

## Adding a 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

---

**Step 1** Choose **User Management > End User**, then click **Add New**. The End User Configuration window appears.



- Step 2** In the User Information pane of this window, enter the following:
- User ID—Enter the end user identification name. Cisco Unified Communications Manager does not permit modifying the user ID after it is created. You may use the following special characters: =, +, <, >, #, ;, \, , " , and blank spaces.  
**Example:**  *johndoe*
  - Password and Confirm Password—Enter five or more alphanumeric or special characters for the end user password. You may use the following special characters: =, +, <, >, #, ;, \, , " , and blank spaces.
  - Last Name—Enter the end user last name. You may use the following special characters: =, +, <, >, #, ;, \, , " , and blank spaces.  
**Example:**  *doe*
  - Telephone Number—Enter the primary directory number for the end user. End users can have multiple lines on their phones.  
**Example:** 26640 (John Doe’s internal company telephone number)
- Step 3** Click **Save**.
- Step 4** Proceed to the section [Configuring the Phone, page F-3](#).
- 

## Configuring the Phone

First, perform the following procedure to identify the user’s phone model and protocol:

### Procedure To Select Phone Model and Protocol

---

- Step 1** From Cisco Unified Communications Manager administration, choose **Device > Phone >**.
- Step 2** Click **Add New**.
- Step 3** Select the user’s phone model from the Phone Type drop-down list, then click **Next**.
- Step 4** Select the device protocol (SCCP or SIP) from the drop-down list, then click **Next**. The Phone Configuration window appears.
- 

### Procedure to Configure Phone

On the Phone Configuration window, you can use the default values for most of the fields.

The following procedure describes how to configure the required fields and some key additional fields:

---

- 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. Make sure that the value comprises 12 hexadecimal characters.  
**Example:** 00127F576611 (MAC address on john doe’s phone)

- **Description**—This is an optional field in which you can enter a useful description, such as *john doe's phone*. This will help you if you need to search on information about this user.
- **Device Pool**—Choose the device pool to which you want this phone assigned. The device pool defines sets of common characteristics for devices, such as region, date/time group, softkey template, and MLPP information.




---

**Note** Device Pools are defined on the Device Pool Configuration window of Cisco Unified Communications Server Administration (**System > Device Pool**).

---

- **Phone Button Template**—Choose the appropriate phone button template from the drop-down list. The phone button template determines the configuration of buttons on a phone and identifies which feature (line, speed dial, and so on) 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 field(s) in conjunction with the **Find** button to find all configured phone button templates and their current settings.

---

- **Softkey Template**—Choose the appropriate softkey template. The softkey template determines the configuration of the softkeys on Cisco Unified IP Phones. Leave this field blank if the common device configuration contains the assigned softkey template.




---

**Note** Softkey templates are defined on the Softkey Template Configuration window of Cisco Unified Communications Manager Administration (**Device > Device Settings > Softkey Template**). You can use the search field(s) in conjunction with the **Find** button to find all configured softkey templates and their current settings.

---

- **Common Phone Profile**—From the drop-down list box, choose a common phone profile from the list of available common phone profiles.




---

**Note** Common Phone Profiles are defined on the Common Phone Profile Configuration window of Cisco Unified Communications Manager Administration (**Device > Device Settings > Common Phone Profile**). You can use the search field(s) 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.




---

**Note** 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 field(s) 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 non-secure 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. (For SIP Phones only) Also in the Protocol Specific Information pane of this window, choose the applicable SIP Profile from the drop-down list.
- 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 (i.e. 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:
- Display (Internal Caller ID field)—You can enter the first name and last name of the user of this device so that this name will be 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 the check box at right (Update Shared Device Settings) and click the **Propagate Selected** button. (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 user’s name, then click **Add Selected**. The user’s 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 your 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 (i.e. *doe* for the last name).
  - Click on the user ID (i.e. *john**doe*). 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 the **Go** button next to the “Back to User” Related link in the upper-right corner of the screen.
- l. Proceed to [Performing Final End User Configuration Steps, page F-8](#).

# Performing Final End User Configuration Steps

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 (i.e. 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 the Enable Mobility box.

**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**.

---







## INDEX

---

### Symbols

? button [1-3](#)

---

### Numerics

10/100 PC port [3-3](#)

10/100 SW port [3-3](#)

---

### A

abbreviated dialing [5-2, B-1](#)

AC adapter, connecting to [3-5](#)

access, to phone settings [3-11, 4-1](#)

access port

    connecting [3-5](#)

    purpose [3-3](#)

adding

    Cisco Unified IP Phones manually [2-9](#)

    Cisco Unified IP Phones using auto-registration [2-8](#)

    Cisco Unified IP Phones using auto-registration with TAPS [2-9](#)

    Cisco Unified IP Phones using BAT [2-10](#)

    users to Cisco Unified Communications Manager [5-12](#)

adjusting, phone placement [3-8](#)

Admin. VLAN Id option [4-6](#)

Alternate TFTP option [4-7](#)

attendant console [B-3](#)

audience, for this document [1-xiii](#)

authenticated call [1-11](#)

authentication [1-7, 3-10](#)

Authentication URL option [4-7](#)

auto answer [5-2, B-1](#)

AutoAttendant [B-3](#)

auto-pickup [5-2](#)

auto-registration

    using [2-8](#)

    using with TAPS [2-9](#)

auxiliary VLAN [2-3](#)

---

### B

barge [1-11, 5-3, B-1](#)

BAT (Bulk Administration Tool) [2-10](#)

block external to external transfer [5-3](#)

BootP [1-4](#)

BOOTP Server option [4-4](#)

Bootstrap Protocol (BootP) [1-4](#)

Busy Lamp Field (BLF) Pickup [B-1](#)

Busy Lamp Field (BLF) speed dial [5-3](#)

button

    ? (help) [1-3](#)

    directories [1-3](#)

    headset [1-3](#)

    line [1-3](#)

    messages [1-3](#)

    mute [1-3](#)

    navigation [1-3](#)

    services [1-3](#)

    settings [1-3](#)

    speaker [1-3](#)

    speed dial [1-3](#)

    volume [1-3](#)

**C**

- call
  - authenticated [1-11](#)
  - encrypted [1-11](#)
- call back [B-1](#)
- call display restrictions [5-3, B-1](#)
- caller ID [5-4, B-2](#)
- call forward [5-3](#)
- call forward all [B-1](#)
- call forward busy [B-1](#)
- call forward display, configuring [5-4](#)
- call forward no answer [B-2](#)
- call logs [B-3](#)
- CallManager Configuration menu [4-10](#)
- call park [5-3, B-2](#)
- call pickup [5-4, B-2](#)
- call statistics [B-3](#)
- Call Statistics screen [6-10](#)
- call statistics screen [6-1](#)
- call waiting [5-4, B-2](#)
- CAPF [6-12, 6-14](#)
- CAPF (Certificate Authority Proxy Function) [1-10, 3-10](#)
- caution, mobile phone interference [1-1](#)
- ccharge [B-1](#)
- CDP [1-4](#)
- certificate icon [6-13](#)
- certificate trust list file
  - See CTL file
- Cisco Call Back [5-4](#)
- Cisco Discovery Protocol
  - See CDP
- Cisco Unified Communications Manager
  - adding phone to database of [2-7](#)
  - attendant console [B-3](#)
  - AutoAttendant [B-3](#)
  - interactions with [2-2](#)
  - verifying settings [8-4](#)
- Cisco Unified Communications Manager Administration
  - adding phones using [2-9](#)
  - adding telephony features using [5-2](#)
  - Cisco Unified Communications Manager Assistant [B-3](#)
  - Cisco Unified IP Phone
    - adding manually to Cisco Unified Communications Manager [2-9](#)
    - adding to Cisco Unified Communications Manager [2-7](#)
    - cleaning [8-17](#)
    - configuration checklist [1-13](#)
    - configuring user services [5-11](#)
    - installation checklist [1-16](#)
    - installation overview [1-16](#)
    - installation procedure [3-5](#)
    - modifying phone button templates [5-10](#)
    - mounting to wall [3-8](#)
    - registering [2-7](#)
    - registering with Cisco Unified Communications Manager [2-8, 2-9, 2-10](#)
    - resetting [8-13](#)
    - supported networking protocols [1-4](#)
    - technical specifications [E-1](#)
    - troubleshooting [8-1](#)
    - using LDAP directories [5-9](#)
    - web page [7-1](#)
  - Cisco Unified IP Phone 7940G
    - features [1-2](#)
    - figure [1-2](#)
  - Cisco Unified IP Phone 7960G
    - features [1-2](#)
    - figure [1-2](#)
  - Cisco Unified IP Phone Expansion Module 7914
    - attaching [3-7](#)
    - statistics [6-2, 6-9](#)
    - troubleshooting [8-12](#)
  - cleaning the Cisco Unified IP Phone [8-17](#)
  - codec
    - mismatch [8-10](#)
    - wideband [1-11](#)
  - Communications Manager 1-5 option [4-6](#)

conference [5-4, B-2](#)  
 configurable call forward display [5-4](#)  
 configuration file  
     creating [8-5](#)  
     overview [2-5](#)  
     XmlDefault.cnf.xml [2-5](#)  
 configuration settings, restoring [8-13](#)  
 configuring  
     from a Cisco Unified IP Phone [4-2](#)  
     LDAP directories [5-9](#)  
     personal directories [5-9](#)  
     phone button templates [5-10](#)  
     softkey templates [5-11](#)  
     startup network settings [3-10](#)  
     user features [5-12](#)  
 connecting  
     handset [3-5](#)  
     headset [3-5](#)  
     to AC adapter [3-5](#)  
     to a computer [3-5](#)  
     to the network [3-5](#)  
 connecting IP phones to other IP phones (daisy chaining) [8-10](#)  
 corporate directories [B-3](#)  
 CTL file  
     deleting [8-13](#)  
     MD5 hash [6-2](#)  
     option on CTL File menu [6-12](#)  
     requesting [2-6](#)  
     unlocking [6-13](#)  
 CTL File menu  
     about [6-12](#)  
     CAPF option [6-12](#)  
     Communications Manager/TFTP option [6-12](#)  
     Communications Manager option [6-13](#)  
     CTL File option [6-12](#)  
     displaying [6-12](#)  
     TFTP Server option [6-13, 6-14](#)

---

## D

data VLAN [2-3](#)  
 Debug Display web page [7-2, 7-10](#)  
 Default Router 1-5 option [4-6](#)  
 Default softkey [8-13](#)  
 device authentication [1-9](#)  
 Device Information web page [7-2, 7-3](#)  
 DHCP  
     description [1-4](#)  
     troubleshooting [8-7](#)  
 DHCP Address Released option [4-7](#)  
 DHCP Enabled option [4-7](#)  
 DHCP Server option [4-4](#)  
 directories button [1-3](#)  
 Directories URL option [4-6](#)  
 directory  
     corporate [B-3](#)  
     personal [B-3](#)  
 directory numbers, assigning manually [2-9](#)  
 direct transfer [5-4](#)  
 DNS server  
     troubleshooting [8-8](#)  
     verifying settings [8-4](#)  
 DNS Server 1-5 option [4-6](#)  
 documentation  
     additional [1-xiv](#)  
 documentation, for users [A-2](#)  
 Domain Name option [4-5](#)  
 do not disturb [5-5, B-2](#)  
 Dynamic Host Configuration Protocol  
     See DHCP

---

## E

editing, configuration values [4-3](#)  
 encrypted call [1-11](#)  
 encryption  
     media [1-10](#)

overview [1-7](#)  
 restrictions [1-11](#)

enterprise parameters  
 call forward options [5-13](#)  
 user options web page defaults [5-13](#)

Erase Configuration option [4-7](#)

Erase softkey [8-13](#)

error messages, used for troubleshooting [8-3](#)

Ethernet web page [7-2, 7-7](#)

Expansion Module Stats screen [6-2, 6-9](#)

extension mobility [5-5, B-2](#)

external power [2-4](#)

---

## F

factory reset [8-14](#)

fast dial [B-2](#)

features  
 configuring on phone, overview [1-7](#)  
 configuring with Cisco Unified Communications Manager, overview [1-6](#)  
 informing users about, overview [1-7](#)

figure  
 Cisco Unified IP Phone 7940G [1-2](#)  
 Cisco Unified IP Phone 7960G [1-2](#)  
 Cisco Unified IP Phone 7960G/7940G cable connections [3-6](#)  
 Cisco Unified IP Phone wall mount [3-9](#)

file authentication [1-9](#)

Firmware Versions screen [6-2, 6-8](#)

footstand  
 adjustment knob [1-3](#)  
 using to adjust phone height [3-8](#)

---

## G

group call pickup [5-5, B-2](#)

---

## H

handset  
 connecting [3-3, 3-5](#)  
 light strip [1-2](#)

headset  
 audio quality [3-4](#)  
 button [1-3](#)  
 connecting [3-4](#)  
 disabling [3-4](#)  
 quality [3-4](#)  
 using [3-3, 3-4](#)

headset port [3-5](#)

height, adjusting [3-8](#)

hold [5-5, B-2](#)

hook switch contacts [8-11](#)

Host Name option [4-5](#)

HTTP [1-4](#)

Hypertext Transfer Protocol  
 See HTTP

---

## I

icon  
 lock [1-11](#)  
 padlock [1-11](#)  
 shield [1-11](#)

Idle URL option [4-7](#)

Idle URL Time option [4-7](#)

image authentication [1-9](#)

immediate divert [5-6, B-2](#)

Information URL option [4-6](#)

installing  
 network requirements [3-2](#)  
 preparing [2-7](#)  
 procedure [3-5](#)

interference, mobile phone [1-1](#)

Internet Protocol (IP) [1-4](#)

IP address, troubleshooting [8-4](#)

IP Address option [4-5](#)

## J

join [5-6](#), [B-2](#)

## K

keypad [1-3](#)

## L

language overlays [C-1](#)

LDAP directories, using with Cisco Unified IP Phone [5-9](#)

light strip [1-2](#)

line button [1-3](#)

Locale Installer [C-1](#)

localization

    Installing the Cisco Unified Communications Manager  
    Locale Installer [C-1](#)

    phone button overlays for [C-1](#)

locally significant certificate (LSC) [6-12](#)

lock icon [1-11](#)

loopback condition [8-12](#)

## M

MAC address [2-12](#)

MAC Address option [4-5](#)

malicious caller identification (MCID) [5-6](#)

malicious call ID [B-2](#)

manufacturing installed certificate (MIC) [1-9](#), [6-12](#)

media encryption [1-10](#)

meet-me conference [5-6](#), [B-2](#)

messages button [1-3](#)

Messages URL option [4-6](#)

message waiting [5-6](#)

message waiting indicator [B-2](#)

MIC [1-9](#)

MLPP [B-2](#)

mobile phone, interference [1-1](#)

Model Information screen [6-1](#)

multilevel precedence and preemption [B-2](#)

multilevel precedence and preemption (MLPP) [5-6](#)

multiple calls per line [B-2](#)

music on hold [B-2](#)

music-on-hold [5-6](#)

mute [B-2](#)

mute button [1-3](#)

## N

native VLAN [2-3](#)

navigation button [1-3](#)

network configuration, resetting [4-7](#), [8-13](#)

Network Configuration menu

    about [4-1](#)

    Admin. VLAN Id option [4-6](#)

    Alternate TFTP option [4-7](#)

    Authentication URL option [4-7](#)

    BOOTP Server option [4-4](#)

    Communications Manager 1-5 option [4-6](#)

    Default Router 1-5 option [4-6](#)

    DHCP Address Released option [4-7](#)

    DHCP Enabled option [4-7](#)

    DHCP Server option [4-4](#)

    Directories URL option [4-6](#)

    displaying [4-1](#)

    DNS Server 1-5 option [4-6](#)

    Domain Name option [4-5](#)

    editing options [4-3](#)

    editing values [4-2](#)

    Erase Configuration option [4-7](#)

    Host Name option [4-5](#)

    Idle URL option [4-7](#)

    Idle URL Time option [4-7](#)

    Information URL option [4-6](#)

    IP Address option [4-5](#)

- locking options [4-2](#)
- MAC Address option [4-5](#)
- Messages URL option [4-6](#)
- Network Locale option [4-8](#)
- Network Locale Version option [4-8](#)
- Operational VLAN Id option [4-6](#)
- PC Port Configuration URL option [4-8](#)
- PC Port Disabled option [4-7](#)
- Proxy Server URL option [4-7](#)
- Services URL option [4-7](#)
- Subnet Mask option [4-5](#)
- SW Port Configuration option [4-8](#)
- TFTP Server 1 option [4-5](#)
- TFTP Server 2 option [4-8](#)
- unlocking options [4-2](#)
- User Locale Option [4-8](#)
- User Locale Version option [4-8](#)
- Network Configuration web page [7-2, 7-4](#)
- network connection, moving [8-10](#)
- network connections, access port [3-3](#)
- network connectivity, verifying [8-3](#)
- networking protocol
  - BootP [1-4](#)
  - CDP [1-4](#)
  - DHCP [1-4](#)
  - HTTP [1-4](#)
  - IP [1-4](#)
  - RTP [1-4](#)
  - SCCP [1-5](#)
  - SIP [1-4](#)
  - TCP [1-5](#)
  - TFTP [1-5](#)
  - UDP [1-5](#)
- networking protocols, supported [1-4](#)
- Network Locale option [4-8](#)
- Network Locale Version option [4-8](#)
- network outages, identifying [8-7](#)
- network port
  - connecting to [3-5](#)

- purpose [3-3](#)
- network requirements, for installing [3-2](#)
- network settings, startup configuration [3-10](#)
- network statistics [6-7, 7-7](#)
- Network Statistics screen [6-2, 6-7](#)

---

## O

- on hook call transfer [5-6](#)
- on-hook dialing/pre-dial [B-2](#)
- Operational VLAN Id option [4-6](#)
- other group pickup [5-6](#)

---

## P

- padlock icon [1-11, 4-2](#)
- PC Port Configuration option [4-8](#)
- PC Port Disabled option [4-7](#)
- personal directories, configuring [5-9](#)
- personal directory [B-3](#)
- phone button templates
  - 7940, default template [5-10](#)
  - 7960, default template [5-10](#)
  - modifying [5-10](#)
- phone screen [1-2](#)
- physical connection, verifying [8-6](#)
- plugging in Cisco Unified IP Phone [3-5](#)
- PoE [2-4](#)
- Port 1 (Network) web page [7-2, 7-7](#)
- Port 2 (Access) web page [7-2, 7-7](#)
- Port 3 (Phone) web page [7-2, 7-7](#)
- power
  - external [2-4](#)
  - outage [2-4](#)
  - PoE [2-4](#)
- power cycle [8-5, 8-8](#)
- power over Ethernet
  - See PoE

power sources [2-4](#)  
 presence-enabled directories [5-6](#)  
 privacy [5-7, B-2](#)  
 Proxy Server URL option [4-7](#)

---

## Q

QRT [B-2](#)  
 QRT softkey [5-7, 8-15](#)  
 quality reporting tool [B-2](#)  
 Quality Reporting Tool (QRT) [5-7, 8-15](#)

---

## R

Real-Time Transport Protocol  
     See RTP  
 redial [5-7, B-2](#)  
 resetting  
     basic [8-13](#)  
     Cisco Unified IP phone [8-13](#)  
     continuously [8-6](#)  
     intentionally [8-8](#)  
     methods [8-13](#)  
     to factory values [8-14](#)  
 Restore softkey [8-13](#)  
 resume [B-2](#)  
 ring activity [5-7](#)  
 ringer, indicator for [1-2](#)  
 RTP [1-4](#)

---

## S

SCCP, description [1-5](#)  
 SDK compliance [B-3](#)  
 secure SRST reference [1-9](#)  
 security  
     CAPF (Certificate Authority Proxy Function) [1-10, 3-10](#)  
     configuring on phone [3-10](#)

device authentication [1-9](#)  
 file authentication [1-9](#)  
 image authentication [1-9](#)  
 Locally Significant Certificate (LSC) [3-10](#)  
 manufacturing installed certificate (MIC) [1-9](#)  
 media encryption [1-10](#)  
 secure SRST reference [1-9](#)  
 security profiles [1-10](#)  
 signaling authentication [1-9](#)  
 signaling encryption [1-10](#)  
 troubleshooting [8-9](#)  
 Security Configuration menu  
     about [6-12](#)  
     CAPF option [6-12](#)  
     CTL File option [6-12](#)  
     LSC option [6-12](#)  
     MIC option [6-12](#)  
     Security Mode option [6-12](#)  
     Trust List option [6-12](#)  
     Web Access option [6-12](#)  
 security profiles [1-10](#)  
 select [B-2](#)  
 services  
     configuring for users [5-11](#)  
     description [5-7](#)  
     subscribing to [5-11](#)  
 services button [1-3](#)  
 Services URL button [5-7](#)  
 Services URL option [4-7](#)  
 settings button [1-3](#)  
 Settings menu access [3-11, 4-1](#)  
 shared line [5-7, B-2](#)  
 shield icon [1-11](#)  
 signaling authentication [1-9](#)  
 signaling encryption [1-10](#)  
 SIP [1-4](#)  
 softkey buttons [1-3](#)  
 softkey templates, configuring [5-11](#)  
 speaker button

- description [1-3](#)
- disabling [3-3](#)
- speed dial button [1-3](#)
- speed dialing [5-2, 5-7, B-3](#)
- SRST
  - description [4-11](#)
  - designation [6-14, 7-5](#)
  - secure reference [1-9](#)
- Stack Statistics web page [7-2, 7-10](#)
- startup problems [8-1](#)
- startup process
  - accessing TFTP server [2-6](#)
  - configuring VLAN [2-6](#)
  - contacting Cisco Unified Communications Manager [2-7](#)
  - loading stored phone image [2-6](#)
  - obtaining IP address [2-6](#)
  - obtaining power [2-6](#)
  - requesting configuration file [2-7](#)
  - requesting CTL file [2-6](#)
  - understanding [2-6](#)
  - verifying [3-9](#)
- statistics
  - call [6-10](#)
  - network [6-7, 7-7](#)
  - stack [7-10](#)
  - streaming [7-11](#)
- statistics, network [6-7](#)
- Status menu [6-1, 6-2](#)
- status messages [6-3](#)
- Status Messages screen [6-2, 6-3](#)
- Status Messages web page [7-3, 7-10, 7-11](#)
- Stream 0 web page [7-3](#)
- Stream 1 web page [7-3, 7-11](#)
- Stream 2 web page [7-3](#)
- streaming statistics [7-11](#)
- Subnet Mask option [4-5](#)
- Survivable Remote Site Telephony
  - See* SRST

- switch
  - Cisco Catalyst [2-3](#)
  - internal Ethernet [2-3](#)
  - loopback condition [8-12](#)
- SW Port Configuration option [4-8](#)

---

## T

- TAPS (Tool for Auto-Registered Phones Support) [2-9](#)
- TCP [1-5](#)
- technical specifications, for Cisco Unified IP Phone [E-1](#)
- telephony features
  - abbreviated dialing [5-2](#)
  - auto answer [5-2](#)
  - auto-pickup [5-2](#)
  - barge [1-11, 5-3](#)
  - block external to external transfer [5-3](#)
  - Busy Lamp Field (BLF) Pickup [B-1](#)
  - Busy Lamp Field (BLF) speed dial [5-3](#)
  - call display restrictions [5-3](#)
  - caller ID [5-4](#)
  - call forward [5-3](#)
  - call park [5-3](#)
  - call pickup [5-4](#)
  - call waiting [5-4](#)
  - Cisco Call Back [5-4](#)
  - conference [5-4](#)
  - configurable call forward display [5-4](#)
  - direct transfer [5-4](#)
  - do not disturb [5-5](#)
  - extension mobility [5-5](#)
  - group call pickup [5-5](#)
  - hold [5-5](#)
  - immediate divert [5-6](#)
  - join [5-6](#)
  - malicious caller identification (MCID) [5-6](#)
  - meet-me conference [5-6](#)
  - multilevel precedence and preemption (MLPP) [5-6](#)
  - music-on-hold [5-6](#)



- on hook call transfer [5-6](#)
  - other group pickup [5-6](#)
  - presence-enabled directories [5-6](#)
  - privacy [5-7](#)
  - redial [5-7](#)
  - ring activity [5-7](#)
  - services [5-7](#)
  - Services URL button [5-7](#)
  - shared line [5-7](#)
  - speed dialing [5-7](#)
  - Time-of-Day Routing [5-8](#)
  - transfer [5-8](#)
  - video mode [5-8](#)
  - video support [5-8](#)
  - voice messaging system [5-8](#)
  - templates, phone button
    - 7940, default [5-10](#)
    - 7960, default [5-10](#)
  - TFTP
    - description [1-5](#)
    - troubleshooting [8-3](#)
  - TFTP Server 1 option [4-5](#)
  - TFTP Server 2 option [4-8](#)
  - time, displayed on phone [3-2](#)
  - Time-of-Day Routing [5-8](#)
  - TLS [1-5, 2-5](#)
  - transfer [5-8, B-3](#)
  - Transmission Control Protocol
    - See TCP
  - Transport Layer Security
    - See TLS
  - Trivial File Transfer Protocol
    - See TFTP
  - troubleshooting
    - Cisco Unified Communications Manager settings [8-4](#)
    - Cisco Unified IP Phone [8-1](#)
    - Cisco Unified IP Phone Expansion Module 7914 [8-12](#)
    - DHCP [8-7](#)
    - DNS [8-8](#)
    - DNS settings [8-4](#)
    - DTMF delay [8-10](#)
    - gaps in voice calls [8-11](#)
    - hook switch contacts [8-11](#)
    - IP addressing and routing [8-4](#)
    - loopback condition [8-12](#)
    - network connectivity [8-3](#)
    - network outages [8-7](#)
    - phones resetting [8-8, 8-10](#)
    - physical connection [8-6](#)
    - security [8-9](#)
    - services on Cisco Unified Communications Manager [8-4](#)
    - sound sample mismatch [8-11](#)
    - TFTP settings [8-3](#)
    - VLAN configuration [8-7](#)
    - voice quality [8-10](#)
  - Trust List menu
    - CAPF option [6-14](#)
    - Communications Manager/TFTP option [6-14](#)
    - Communications Manager option [6-14](#)
    - description [6-12](#)
    - displaying [6-14](#)
    - SRST option [6-14](#)
- 
- ## U
- UDP [1-5](#)
  - Unlock softkey [6-13](#)
  - User Datagram Protocol
    - See UDP
  - User Locale option [4-8](#)
  - User Locale Version option [4-8](#)
  - User Options web page
    - description [5-12](#)
    - giving users access to [5-12, A-1](#)
  - user options web page
    - call forward settings [5-12](#)
  - users

accessing voice messaging system [A-3](#)  
 adding to Cisco Unified Communications Manager [5-12](#)  
 configuring personal directories [A-3](#)  
 documentation for [A-2](#)  
 how they get support [A-1](#)  
 required information [A-1](#)  
 subscribing to services [A-2](#)  
 user settings, resetting [8-13](#)

---

## V

video [B-3](#)  
 video mode [5-8](#)  
 video support [5-8](#)

### VLAN

auxiliary, for voice traffic [2-3](#)  
 configuring for voice networks [2-3](#)  
 native, for data traffic [2-3](#)  
 verifying [8-7](#)  
 voice messaging system [B-3](#)  
     feature description [5-8](#)  
 voice messaging system, accessing [A-3](#)  
 voice quality metrics [B-3](#)  
 voice VLAN [2-3](#)  
 volume button [1-3](#)

---

## W

wall mounting, Cisco Unified IP Phone [3-8](#)  
 web page  
     about [7-1](#)  
     accessing [7-2](#)  
     Debug Display [7-2, 7-10](#)  
     Device Information [7-2, 7-3](#)  
     disabling access to [7-3](#)  
     Ethernet [7-2, 7-7](#)  
     Network Configuration [7-4](#)  
     Network Configuration web page [7-2](#)

Port 1 (Network) [7-2, 7-7](#)  
 Port 2 (Access) [7-2, 7-7](#)  
 Port 3 (Phone) [7-2, 7-7](#)  
 preventing access to [7-3](#)  
 Stack Statistics [7-2, 7-10](#)  
 Status Messages [7-3, 7-10, 7-11](#)  
 Stream 0 [7-3](#)  
 Stream 1 [7-3, 7-11](#)  
 Stream 2 [7-3](#)  
 wideband codec [1-11](#)

---

## X

XmlDefault.cnf.xml [2-5](#)

## Free Manuals Download Website

<http://myh66.com>

<http://usermanuals.us>

<http://www.somanuals.com>

<http://www.4manuals.cc>

<http://www.manual-lib.com>

<http://www.404manual.com>

<http://www.luxmanual.com>

<http://aubethermostatmanual.com>

Golf course search by state

<http://golfingnear.com>

Email search by domain

<http://emailbydomain.com>

Auto manuals search

<http://auto.somanuals.com>

TV manuals search

<http://tv.somanuals.com>