



Cisco Unified Wireless IP Phone 7925G Administration Guide for Cisco Unified Communications Manager 7.0(1)

Americas Headquarters

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

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

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

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

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

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

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

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

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

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

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; 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, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, 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. (0809R)

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

Cisco Unified Wireless IP Phone 7925G Administration Guide for Cisco Unified Communications Manager 7.0(1)
© 2008 Cisco Systems, Inc. All rights reserved.



The Bluetooth word mark and logo are registered trademarks owned by Bluetooth SIG, Inc., and any use of such marks by Cisco Systems, Inc., is under license.



CONTENTS

Preface xi

Overview	xi
Audience	xi
Organization	xii
Related Documentation	xiii
Obtaining Documentation and Submitting a Service Request	xiii
Cisco Product Security Overview	xiii
Document Conventions	xiv

CHAPTER 1

Overview of the Cisco Unified Wireless IP Phone 7925G	1-1
Understanding the Cisco Unified Wireless IP Phone 7925G	1-1
Bluetooth Technology	1-2
Handsfree Profile	1-2
Pairing with Headsets	1-3
Features Supported on the Cisco Unified Wireless IP Phone 7925G	1-6
Feature Overview	1-7
Telephony Features	1-7
Network Settings Configuration	1-7
Feature Information for Users	1-8
Understanding Security Features for Cisco Unified IP Phones	1-8
Overview of Supported Security Features	1-10
Understanding Security Profiles	1-12
Identifying Authenticated, Encrypted, and Protected Phone Calls	1-12
Establishing and Identifying Protected Calls	1-13
Security Restrictions	1-13
Overview of Configuring and Installing the Cisco Unified Wireless IP Phone 7925G	1-14
Configuring the Cisco Unified Wireless IP Phone 7925G in Cisco Unified Communications Manager	1-14
Installing the Cisco Unified Wireless IP Phone 7925G	1-15

CHAPTER 2

Overview of the VoIP Wireless Network	2-1
Understanding the Wireless LAN	2-1
Understanding WLAN Standards and Technologies	2-3
802.11 Standards for WLAN Communications	2-3

- Radio Frequency Ranges 2-4
- 802.11 Data Rates, Tx Power, Ranges, and Decibel Tolerances 2-4
- Wireless Modulation Technologies 2-5
- AP, Channel, and Domain Relationships 2-6
- WLANs and Roaming 2-7
- Bluetooth Wireless Technology 2-8
 - Pairing Headsets 2-8
- Components of the VoIP Wireless Network 2-9
 - Networking Protocols Used with Cisco Unified Wireless IP Phones 2-9
 - Interacting with Cisco Unified Wireless APs 2-11
 - Associating to APs 2-12
 - Voice QoS in a Wireless Network 2-12
 - Interacting with Cisco Unified Communications Manager 2-14
 - Phone Configuration Files and Profile Files 2-14
 - Interacting with the Dynamic Host Configuration Protocol Server 2-15
- Security for Voice Communications in WLANs 2-16
 - Authentication Methods 2-16
 - Authenticated Key Management 2-18
 - Encryption Methods 2-18
 - Choosing AP Authentication and Encryption Methods 2-18
- VoIP WLAN Configuration 2-21
 - Wireless Network Requirements for VoIP 2-21
 - Configuring the Wireless Network for Voice 2-22
 - Configuration Tip for Cisco Aironet APs 2-22
- Site Survey Verification 2-22
 - Performing a Site Survey Verification 2-23
 - Using the Neighbor List Utility 2-23
 - Using the Site Survey Utility 2-24

CHAPTER 3

Setting Up the Cisco Unified Wireless IP Phone 7925G 3-1

- Before You Begin 3-1
 - Network Requirements 3-1
 - Methods for Adding Phones to Cisco Unified Communications Manager 3-2
 - Adding Phones with Auto-Registration 3-3
 - Adding Phones with Auto-Registration and TAPS 3-3
 - Adding Phones with BAT 3-4
 - Adding Phones with Cisco Unified Communications Manager Administration 3-4
 - Device Support 3-5
 - Safety Information 3-5

Battery Safety Notices	3-6
Installing the Cisco Unified Wireless IP Phone 7925G	3-7
Providing Power to the Phone	3-7
Installing or Removing the Phone Battery	3-8
Using the Power Supply to Charge the Phone Battery	3-11
Using the USB Cable and PC to Charge the Battery	3-12
Configuring Wireless LAN Settings for the Cisco Unified Wireless IP Phone 7925G	3-13
Cisco Unified Wireless IP Phone 7925G Web Pages	3-13
Network Profile Menu on the Cisco Unified Wireless IP Phone 7925G	3-13
Using a Headset	3-13
Connecting Headsets	3-14
Using Bluetooth Wireless Headsets	3-14
Audio Quality Subjective to the User	3-15
Using External Devices with Cisco Unified IP Phones	3-15
Powering On the Cisco Unified Wireless IP Phone 7925G	3-15
Active and Standby Phone Modes	3-16
Active Mode	3-16
Standby Mode	3-17
Understanding the Phone Startup Process	3-17

CHAPTER 4**Using the Cisco Unified Wireless IP Phone 7925G Web Pages** 4-1

Setting Up Your PC to Configure the Phones	4-1
Installing the USB Drivers	4-2
Configuring the USB LAN on the PC	4-2
Accessing the Phone Web Page	4-3
Using the USB Cable to Configure Phones	4-4
Updating the Phones Remotely	4-4
Setting Configuration Privileges for the Phone Web Page	4-4
Accessing the Configuration Web Page for a Phone	4-5
Summary Information on the Home Web Page	4-7
Configuring Network Profiles	4-8
Network Profile Settings	4-8
Configuring Wireless Settings in a Network Profile	4-12
Configuring Wireless LAN Security	4-13
Configuring the Authentication Mode	4-14
Setting the Wireless Security Credentials	4-15
Configuring the Username and Password	4-15
Configuring the Pre-shared Key	4-15
Setting Wireless Encryption	4-16

- Installing Authentication Certificates for EAP-TLS Authentication 4-17
- Configuring PEAP 4-22
- Configuring IP Network Settings 4-23
 - Enabling DHCP 4-23
 - Disabling DHCP 4-24
- Configuring the Alternate TFTP Server 4-24
- Configuring Advanced Network Profile Settings 4-25
- Configuring USB Settings 4-26
- Configuring Trace Settings 4-27
- Configuring Wavelink Settings 4-29
- Configuring the Phone Book 4-29
 - Importing and Exporting Contacts 4-30
 - Importing and Exporting CSV Phone Contact Records 4-30
 - Searching the Phone Book Information 4-32
 - Updating Phone Book Information 4-32
 - Adding a Contact 4-32
 - Deleting Contacts 4-33
 - Editing Contact Information 4-33
 - Assigning A Speed-Dial Hot Key to a Contact Number 4-33
- Using System Settings 4-34
 - Viewing Trace Logs 4-34
 - Backup Settings for Phone Configuration 4-34
 - Using Network Profile Templates 4-35
 - Creating a Configuration Template 4-35
 - Importing a Configuration Template 4-37
 - Upgrading Phone Firmware 4-37
 - Changing the Admin Password 4-38
 - Viewing the Site Survey Report on the Web 4-38

CHAPTER 5

Configuring Settings on the Cisco Unified Wireless IP Phone 7925G 5-1

- Accessing Network and Phone Settings 5-1
- Configuring Network Profile Settings 5-2
 - Accessing a Network Profile 5-3
 - Changing the Profile Name 5-3
 - Guidelines for Editing Settings in the Network Profile 5-4
 - Changing Network Configuration Settings 5-4
- Configuring DHCP Settings 5-6
 - Disabling DHCP 5-6
 - Configuring an Alternate TFTP Server 5-7

Changing the Cisco Discovery Protocol Settings	5-7
Erasing the Configuration	5-8
Configuring Wireless Settings for the Network Profile	5-8
Accessing the WLAN Configuration Menu	5-8
Changing WLAN Configuration Settings	5-9
Changing Phone Settings	5-10
Configuring the Security Certificate on the Phone	5-12
Changing the USB Configuration	5-13

CHAPTER 6**Configuring the Phone Using the Wavelink Avalanche Server 6-1**

Before You Begin	6-1
Best Practices	6-2
Assigning the Wavelink Server	6-2
Assigning the Wavelink Server from the Phone	6-2
Assigning the Wavelink Server using the Phone Web Page	6-3
Setting Up and Using the Phone CU	6-3
Assigning Attributes for the Phone	6-3
Defining Custom Names and Custom Values on the Phone	6-4
Defining Custom Parameters from the Phone Web Page	6-4
Installing the Cisco Unified Wireless IP Phone 7925G CU	6-4
Updating Configuration Files	6-5
Configuring Profile Settings	6-6
Configuring USB Settings	6-9
Configuring Trace Settings	6-9
Configuring Wavelink Settings	6-10
Updating the Phone	6-10

CHAPTER 7**Configuring Features, Templates, Services, and Users 7-1**

Configuring Cisco Unified Wireless IP Phones in Cisco Unified Communications Manager	7-1
Telephony Features Available for the Phone	7-2
Specific Configuration Options for the Cisco Unified Wireless IP Phone 7925G	7-13
Configuring Softkey Templates	7-16
Softkey Templates for the Cisco Unified Wireless IP Phone 7925G	7-16
Changing Softkeys in a Template	7-16
Modifying Phone Button Templates	7-17
Setting Up Services	7-17
Configuring Corporate and Personal Directories	7-18

- Configuring Corporate Directories 7-19
- Configuring Personal Directory 7-19
- Adding Users to Cisco Unified Communications Manager 7-19
- Managing the User Options Web Pages 7-20
 - Giving Users Access to the User Options Web Pages 7-20
 - Specifying Options that Appear on the User Options Web Pages 7-21
- Creating Custom Phone Rings 7-21

CHAPTER 8

Viewing Security, Device, Model, Status, and Call Statistics Information on the Phone 8-1

- Viewing Security Information 8-1
 - Accessing the CTL File Screen 8-3
 - Trust List Screen 8-4
- Viewing Device Information 8-4
- Viewing Model Information 8-7
- Viewing the Phone Status Menu 8-8
 - Viewing the Status Messages 8-9
 - Viewing the Current Configuration 8-12
- Viewing Network Statistics 8-12
- Viewing Call Statistics 8-14
- Viewing Firmware Versions 8-16

CHAPTER 9

Monitoring the Cisco Unified Wireless IP Phone Remotely 9-1

- Accessing the Web Page for a Phone 9-1
- Summary Information 9-2
- Network Configuration Information 9-3
- Device Information 9-6
- Wireless LAN Statistics 9-7
- Network Statistics 9-9
- Stream Statistics 9-10

CHAPTER 10

Troubleshooting the Cisco Unified Wireless IP Phone 7925G 10-1

- Resolving Startup and Connectivity Problems 10-1
 - Symptom: Incomplete Startup Process 10-1
 - Symptom: No Association to Cisco Aironet Access Points 10-2
 - Verifying Access Point Settings 10-2
 - Symptom: No Registration to Cisco Unified Communications Manager 10-3
 - Registering the Phone with Cisco Unified Communications Manager 10-4
 - Checking Network Connectivity 10-4

Verifying TFTP Server Settings	10-4
Verifying IP Addresses	10-5
Verifying DNS Settings	10-5
Verifying Cisco Unified Communications Manager Settings	10-5
Cisco Unified Communications Manager and TFTP Services are not Running	10-6
Creating a New Configuration File	10-7
Resolving Voice Quality and Roaming	10-8
Symptom: Cisco Unified Wireless IP Phone Resets Unexpectedly	10-8
Verifying Access Point Settings	10-8
Identifying Intermittent Network Outages	10-8
Verifying DHCP Settings	10-9
Verifying Voice VLAN Configuration	10-9
Verifying that the Phones Have Not Been Intentionally Reset	10-9
Eliminating DNS or Other Connectivity Errors	10-9
Symptom: Audio Problems	10-10
No Audio During a Connected Call	10-10
One-Way Audio During a Connected Call	10-10
Symptom: Improper Roaming and Voice Quality or Lost Connection	10-11
Voice Quality Deteriorates While Roaming	10-11
Delays in Voice Conversation While Roaming	10-11
Phone Loses Connection with Cisco Unified Communications Manager While Roaming	10-11
Phone Does Not Roam Back to Preferred Band	10-12
Monitoring the Voice Quality of Calls	10-12
Using Voice Quality Metrics	10-13
Troubleshooting Tips	10-13
General Troubleshooting Information	10-14
Common Phone Status Messages	10-14
Troubleshooting Tips for the Cisco Unified Wireless IP Phone 7925G	10-16
Logging Information for Troubleshooting	10-17
Using a System Log Server	10-18
Using the Trace Logs on the Unified IP Phone	10-18
Erasing the Local Configuration	10-18

APPENDIX A

Providing Information to Users By Using a Website	A-1
How the Cisco Unified Wireless IP Phone Operates	A-1
How to Care for and Clean the Phone	A-2
How Users Access the Help System on the Phone	A-3
How Users Get Copies of Cisco Unified IP Phone Manuals	A-3
How Users Configure Phone Features and Services	A-4

How Users Access Voice Messages A-4

APPENDIX B

Supporting International Users B-1

Installing the Cisco Unified Communications Manager Locale Installer B-1

Support for International Call Logging B-2

APPENDIX C

Physical and Operating Environment Specifications C-1

APPENDIX D

Checklist for Deploying the Cisco Unified Wireless IP Phone 7925G D-1

Configuring a Wireless Network D-1

Configuration Tip for Cisco Aironet Access Points D-2

Configuring QoS Policies D-3

Access Point Configuration Settings D-3

Controller Settings D-3

Switch Configuration D-4

Configuring the Cisco Unified Wireless IP Phone 7925G in Cisco Unified Communications Manager D-4

Installing the Cisco Unified Wireless IP Phone 7925G D-7

INDEX



Preface

This chapter describes the intended audience, objectives, organization, and lists related documentation. It contains the following sections:

- [Overview, page xi](#)
- [Audience, page xi](#)
- [Organization, page xii](#)
- [Related Documentation, page xiii](#)
- [Obtaining Documentation and Submitting a Service Request, page xiii](#)

Overview

Cisco Unified Wireless IP Phone 7925G Administration Guide provides the information you need to understand, install, configure, and manage the Cisco Unified Wireless IP Phone 7925G on your network. This guide is intended to be used to administer phones running with Cisco Unified Communications Manager Release 4.1, 4.2, 4.3, 5.1, 6.0, 6.1, and 7.0(1).

Audience

Network engineers, system administrators, or telecom engineers should review this guide to learn the steps required to properly set up the Cisco Unified Wireless IP Phone 7925G on the wireless 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 could affect the phone functioning in the network.

Because of the close interaction between the Cisco Unified Wireless IP Phone 7925G and Cisco Unified Communications Manager, these tasks require familiarity with Cisco Unified Communications Manager.

Organization

This guide is organized as follows:

Chapter	Description
Chapter 1, “Overview of the Cisco Unified Wireless IP Phone 7925G”	Provides a conceptual overview and description of the Cisco Unified Wireless IP Phone 7925G and provides an overview of the tasks required prior to installation
Chapter 2, “Overview of the VoIP Wireless Network”	Describes how the IP Phone interacts with other key IP telephony and wireless network protocols and components
Chapter 3, “Setting Up the Cisco Unified Wireless IP Phone 7925G”	Describes how to properly and safely install and configure the Cisco Unified Wireless IP Phone 7925G on your network
Chapter 4, “Using the Cisco Unified Wireless IP Phone 7925G Web Pages”	Describes how to use the Cisco Unified Wireless IP Phone 7925G web pages for initial phone configuration and to update configuration files for the wireless IP phone
Chapter 5, “Configuring Settings on the Cisco Unified Wireless IP Phone 7925G”	Describes how to configure network profiles and phone settings, by using the Settings menu on the wireless IP phone
Chapter 6, “Configuring the Phone Using the Wavelink Avalanche Server”	Describes how to use the Cisco Unified Wireless IP Phone 7925G Configuration Utility on the Wavelink Avalanche server for updating the phone configuration
Chapter 7, “Configuring Features, Templates, Services, and Users”	Provides an overview of procedures for configuring telephony features and adding users to Cisco Unified Communications Manager
Chapter 8, “Viewing Security, Device, Model, Status, and Call Statistics Information on the Phone”	Explains how to view phone security, device, and network information and network and call statistics from the wireless IP phone
Chapter 9, “Monitoring the Cisco Unified Wireless IP Phone Remotely”	Explains how to obtain status information about the phone using the phone web page
Chapter 10, “Troubleshooting the Cisco Unified Wireless IP Phone 7925G”	Provides tips for troubleshooting the wireless IP phone
Appendix A, “Providing Information to Users By Using a Website”	Provides suggestions for setting up a website for providing users with important information about their wireless IP phone
Appendix B, “Supporting International Users”	Provides information about setting up phones in non-English environments
Appendix C, “Physical and Operating Environment Specifications”	Provides technical specifications of the Cisco Unified Wireless IP Phone 7925G
Appendix D, “Checklist for Deploying the Cisco Unified Wireless IP Phone 7925G”	Provides a detailed checklist for deploying the Cisco Unified Wireless IP Phone 7925G

Related Documentation

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

Cisco Unified Wireless IP Phone 7925G

These publications are available at the following URLs:

http://www.cisco.com/en/US/products/hw/phones/ps379/tsd_products_support_series_home.html

- *Cisco Unified Wireless IP Phone 7925G Phone Guide*
- *Cisco Unified Wireless IP Phone 7925G Accessory Guide*
- *Cisco Unified Wireless IP Phone 7925G Installation Guide*
- *Cisco Unified Wireless IP Phone 7925G Datasheet*
- *Regulatory Compliance and Safety Information for Cisco Unified Wireless IP Phone 7920 Series and Peripherals*
- *Open Source License Notices for the Cisco Unified IP Phones 7900 Series*

Cisco Unified Communications Manager Administration

Cisco Unified Communications Manager publications are available at the following URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

Cisco Unified Communications Manager Administration Business Edition

Cisco Unified Communications Manager Business Edition publications are available at the following URL:

http://www.cisco.com/en/US/products/ps7273/tsd_products_support_series_home.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, 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>

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

Cisco Product Security Overview

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

Further information regarding U.S. export regulations may be found at http://www.access.gpo.gov/bis/ear/ear_data.html.

Document Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands and keywords are in boldface .
<i>italic font</i>	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 <code>screen font</code> .
boldface screen font	Information you must enter is in boldface screen font .
<i>italic screen font</i>	Arguments for which you supply values are in <i>italic screen font</i> .
^	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

Overview of the Cisco Unified Wireless IP Phone 7925G

This chapter includes the following sections:

- [Understanding the Cisco Unified Wireless IP Phone 7925G, page 1-1](#)
- [Bluetooth Technology, page 1-2](#)
- [Features Supported on the Cisco Unified Wireless IP Phone 7925G, page 1-6](#)
- [Understanding Security Features for Cisco Unified IP Phones, page 1-8](#)
- [Overview of Configuring and Installing the Cisco Unified Wireless IP Phone 7925G, page 1-14](#)

Understanding the Cisco Unified Wireless IP Phone 7925G

The Cisco Unified Wireless IP Phone 7925G provides wireless voice communication over an IP network. Like traditional analog telephones, you can place and receive phone calls and access features such as hold, transfer, and speed dial. In addition, because the phone connects to your wireless local area network (WLAN), you can place and receive phone calls from anywhere in your wireless environment.

The Cisco Unified Wireless IP Phone 7925G is an 802.11 dual band wireless device that provides comprehensive voice communications in conjunction with Cisco Unified Communications Manager and Cisco Aironet 802.11b/g and Cisco Aironet 802.11a Access Points (APs) in a private business communications network. This phone model, like other network devices, must be configured and managed. This phone encodes G.711a, G.711u, G.729a, G.729ab, G.722/iLBC, and decodes G.711a, G.711b, G.711u, G.729, G.729a, G.729b, and G.729ab. The phone also supports uncompressed wideband (16 bits, 16 kHz) audio.

The Cisco Unified Wireless IP Phone 7925G is hearing aid compatible (HAC) but does not have any TTY features. It also has a centered “dot” or “nib” on the 5 key that is a tactile identifier.

The physical characteristics include:

- Resistance to damage from dropping the phone
- Tolerance of anti-bacterial and alcohol-based wipes
- Latex and lead free
- Resistance against liquid splashes

- Dust resistance
- Shock proof and vibration proof
- USB 1.1 interface

Bluetooth Technology

The Cisco Unified Wireless IP Phone 7925G is a full-feature telephone and a qualified Bluetooth wireless device (Qualified Device ID (QDID) B014396). In addition to basic call-handling features, your phone operates with Bluetooth wireless headsets, including certain handsfree call features.

Bluetooth devices operate in the unlicensed Industrial Scientific Medicine (ISM) band of 2.4GHz. This unlicensed band in most countries includes the frequency range from 2400 to 2483.5 MHz. Synchronous voice channels are provided by using circuit switching and asynchronous data channels are provided by using packet switching.

Bluetooth uses an integrated Adaptive Frequency Hopping (AFH) to avoid interference. Every 625 usec (1/1,000,000 of a second) the channel changes or hops to another frequency within the 2402 to 2480 MHz range. This computes to 1600 hops every second.

On the Cisco Unified Wireless IP Phone 7925G, a Bluetooth module and 802.11 WLAN module co-exist in the phone. This co-existence greatly reduces and avoids radio interference between the Bluetooth and 802.11bg radio.

Bluetooth devices fit into to three different power classes, as shown in [Table 1-1](#).

Table 1-1 Bluetooth Maximum Permitted Power and Range by Class

Class	Maximum Permitted Power (dBm)	Maximum Permitted Power (mW)	Range
Class 1	100 mW	20 dBm	Up to 100 meters
Class 2	2.5 mW	4 dBm	Up to 10 meters
Class 3	1 mW	0 dBm	Up to 1 meter

For more information about WLAN configuration and Bluetooth, see [VoIP WLAN Configuration, page 2-21](#). User-specific information is contained in the *Cisco Unified Wireless IP Phone 7925G User Guide*.

For more information about Bluetooth and hands-free profiles, refer to <http://www.bluetooth.com>.

Handsfree Profile

Your phone supports certain features of the Handsfree Profile, which is a standard set of features that enable users of handsfree devices (such as Bluetooth wireless headsets) to perform certain tasks without having to handle the phone, allowing users to be “handsfree.” For example, instead of pressing **Redial** on your phone, you can redial a number from your Bluetooth wireless headset according to instructions from the headset manufacturer.

These handsfree features apply to Bluetooth wireless headsets used with your Cisco Unified Wireless IP Phone 7925G:

- Redial—Recalls the last number dialed.
- Reject incoming call—Uses the iDivert option to direct the call to voicemail.

- Three-way calling—When there is an active call and another incoming call or call on hold, you may choose to handle the calls in one of two ways:
 - End the active call and answer or resume a waiting call.
 - Put the active call on hold and answer or resume a waiting call.

**Note**

Handsfree devices may differ in how features are activated. Handsfree device manufacturers may also use different terms when referring to the same feature.

For more information on using handsfree features, see the documentation provided by the device manufacturer.

Pairing with Headsets

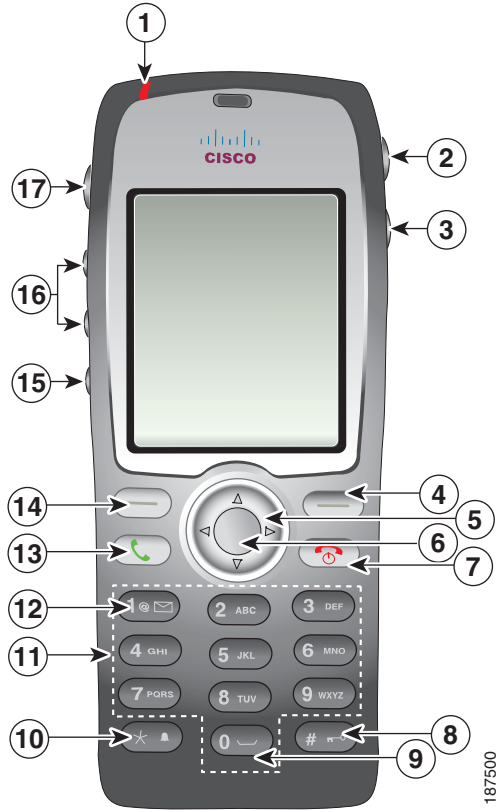
The Cisco Unified Wireless IP Phone 7925G pairs with headsets by using a shared key authentication/encryption method. This process requires confirmation of a PIN specific to the headset, commonly “0000.” The Cisco Unified Wireless IP Phone 7925G can be paired with more than one headset at a time. Pairing is typically performed once for each headset used with the Cisco Unified Wireless IP Phone 7925G. Once pairing is complete, the headset automatically connects to the Cisco Unified Wireless IP Phone 7925G when both devices are powered on and in range.

**Note**

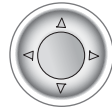















The Cisco Unified Wireless IP Phone 7925G can only be connected to one Bluetooth-enabled headset at a time. Further, the Cisco Unified Wireless IP Phone 7925G only supports communication with Bluetooth wireless technology-enabled devices qualified by the Bluetooth Special Interest Group (SIG).





[Figure 1-1](#) shows the Cisco Unified Wireless IP Phone 7925G. The table that follows describes the functions of the keys on the phone.

Figure 1-1 Cisco Unified Wireless IP Phone 7925G



1	Indicator light (LED)	Provides these indications: <ul style="list-style-type: none"> • Solid red—Phone is connected to AC power source and battery is charging. • Solid green—Phone is connected to AC power source and battery is fully charged. • Fast blinking red—Incoming call. (Phone can be charging or fully charged.) • Slow blinking red—Voice message. (When connected to AC power source, red light displays longer than when phone is using only the battery.) • Slow blinking green—Phone is using only battery power. Phone is registered with the wireless network and is within service coverage area.
2	Headset port cover	Cover for the headset port.
3	Speaker button	Toggles the speaker mode on or off for the phone.
4	Right softkey button	Activates the Options menu for access to the list of softkeys. Sometimes displays a softkey label.

5	Navigation button 	<p>Accesses these menus and lists from the main screen:</p> <p>Directory  </p> <p>Line View  </p> <p>Settings  </p> <p>Services  </p> <p>Allows you to scroll up and down menus to highlight options and to move left and right through phone numbers and text entries.</p>
6	Select button 	<p>Activates the Help menu from the main screen.</p> <p>Allows you to select a menu item, a softkey, a call, or an action.</p>
7	Power/End button (red) 	<p>Turns the phone on or off, silences a ringing call, or ends a connected call.</p> <p>When using menus, acts as a shortcut to return to the main screen.</p>
8	Pound (#) key 	<p>Toggles between locking and unlocking the keypad.</p> <p>Allows you to enter these special characters when you are entering text: # ? () [] { }</p>
9	Zero (0) key 	<p>Enters “0” when dialing a number. Allows you to enter a space or these special characters when you are entering text: +, . ‘ “ _ ~ ’</p> <p>Note When entering text or dialing an international number, use the plus sign (+).</p>
10	Asterisk (*) key 	<p>Toggles between Ring and Vibrate mode.</p> <p>Allows you to enter these special characters when you are entering text: * - / = \ : ;</p>
11	Keypad	<p>Allows you to dial numbers, enter letters, and choose menu items by number.</p> <p>Press and hold key 1 to access your voice messaging system.</p>
12	One (1) key 	<p>Enters “1” when dialing a number. Allows you to access the voice messaging system.</p> <p>Allows you to enter these special characters when you are entering text: ! @ < > \$ % ^ &</p>
13	Answer/Send button (green) 	<p>Allows you to answer a ringing call or, after dialing a number, to place the call.</p>

14	Left softkey button 	Activates the softkey option displayed on the screen. When customized by the phone administrator or user, allows direct access to the Phone Book or voice messages.
15	Mute button 	Toggles the mute feature on or off.
16	Volume button 	<p>When the phone is idle, allows you to control the ring volume, turn on the vibrate option, or turn off the ring.</p> <p>When an incoming call is ringing, allows you to press this button once to silence the ring for the call.</p> <p>During a call, allows you to control the speaker volume for the handset, headset, and speaker mode.</p>
17	Application button 	Configurable button that is used with XML applications, such as Push to Talk or Directory services. See “Setting Up Services” section on page 7-17.

Related Topics

- [Features Supported on the Cisco Unified Wireless IP Phone 7925G, page 1-6](#)
- [Overview of Configuring and Installing the Cisco Unified Wireless IP Phone 7925G, page 1-14](#)

Features Supported on the Cisco Unified Wireless IP Phone 7925G

The Cisco Unified Wireless IP Phone 7925G functions much like traditional IP phones allowing you to place and receive telephone calls while connected to the wireless LAN. In addition to traditional phone features, the Cisco Unified Wireless IP Phone includes features that enable you to administer and monitor the phone as a network device.

**Caution**

This product is not a medical device and may use an unlicensed frequency band that is susceptible to interference from other devices or equipment.

This section provides information about these topics:

- [Feature Overview, page 1-7](#)
- [Telephony Features, page 1-7](#)
- [Understanding Security Profiles, page 1-12](#)
- [Network Settings Configuration, page 1-7](#)
- [Feature Information for Users, page 1-8](#)

Feature Overview

The Cisco Unified Wireless IP Phone 7925G provides traditional telephony functionality, such as call forwarding and transferring, call pickup, redialing, speed dialing, conference calling, and voice messaging system access, as well as these features:

- Bluetooth Class 2 technology for headsets that support Bluetooth
- Six-line appearance
- Adjustable ring and volume levels
- Adjustable display brightness and time outs
- Auto-detection of headset and auto-answer from the headset
- Wireless web access to your phone number and the corporate directory
- Access to network data, XML applications, and web-based services
- Online customizing of phone features and services from the User Options web pages
- An online help system that displays information on the phone screen

Related Topics

- [Configuring Network Profiles, page 4-8](#)
- [Configuring Features, Templates, Services, and Users, page 7-1](#)

Telephony Features

You can use Cisco Unified Communications Manager Administration to set up phone registration criteria and calling search spaces, to configure corporate directories and services, and to modify phone button templates. See the “[Telephony Features Available for the Phone](#)” section on [page 7-2](#) and *Cisco Unified Communications Manager Administration Guide* for additional information.

For more information about the Cisco Unified Communications Manager Administration, refer to Cisco Unified Communications Manager documentation suite at http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

You can also use the context-sensitive help available within the application for guidance.

Related Topic

- [Telephony Features Available for the Phone, page 7-2](#)

Network Settings Configuration

Like other network devices, you must configure IP phones to access Cisco Unified Communications Manager and the rest of the IP network using the wireless LAN. There are two methods for configuring network settings such as DHCP, TFTP, and for configuring wireless settings for the phone.

- Cisco Unified Wireless IP Phone 7925G web pages
- Network Profiles menu on the Cisco Unified Wireless IP Phone 7925G

You can access the configuration web pages by using a browser from your PC. For more information, see [Using the Cisco Unified Wireless IP Phone 7925G Web Pages, page 4-1](#).

You can also configure network settings on the phone itself. For more information about configuring features from the phone, see [Chapter 5, “Configuring Settings on the Cisco Unified Wireless IP Phone 7925G.”](#)

Because the Cisco Unified Wireless IP Phone is a network device, you can obtain detailed status information about it. This information can assist you in troubleshooting problems that users might encounter when using their IP phones. See [Chapter 9, “Monitoring the Cisco Unified Wireless IP Phone Remotely,”](#) for tips on using this information.

Related Topics

- [Using the Cisco Unified Wireless IP Phone 7925G Web Pages, page 4-1](#)
- [Configuring Settings on the Cisco Unified Wireless IP Phone 7925G, page 5-1](#)
- [Monitoring the Cisco Unified Wireless IP Phone Remotely, page 9-1](#)

Feature Information for Users

If you are a system administrator, you are the primary source of information for Cisco Unified Wireless 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 Wireless IP Phone 7925G 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_maintain_and_operate.html

From this site, you can view additional phone documentation.

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

For a summary of the key information that you can provide to phone users, see [Appendix A, “Providing Information to Users By Using a Website.”](#)



Note

The radio frequency (RF) for the Cisco Unified Wireless IP Phone 7925G is configured for a specific regulatory domain. If users attempt to use this phone outside of the regulatory domain, the phone will not function properly and they might violate local regulations.

Related Topic

- [Providing Information to Users By Using a Website, page A-1](#)

Understanding Security Features for Cisco Unified IP Phones

Implementing security in a wireless network protects against data tampering to Cisco Unified Communications Manager data, call signaling, and media stream. It also reduces the chances for identity theft. To reduce the threats, the Cisco wireless LAN (WLAN) provides options for user authentication with servers and for encrypting communications streams between phones and network devices.

For information about supported security options for the Cisco Unified Wireless IP Phone 7925G, see the [“Authentication Methods” section on page 2-16.](#)

For information about security features supported by Cisco Unified Communications Manager and Cisco Unified IP Phones, see the [“Understanding Security Features for Cisco Unified IP Phones”](#) section on page 1-8.

Table 1-2 provides additional information about security topics.

Table 1-2 Cisco Unified IP Phone and Cisco Unified Communications Manager Security Topics

Topic	Reference
Detailed explanation of security, including set up, configuration, and troubleshooting information for Cisco Unified Communications Manager and Cisco Unified IP Phones	Refer to <i>Cisco Unified Communications Manager Security Guide</i>
Security features supported on the Cisco Unified IP Phone	See the “Understanding Security Features for Cisco Unified IP Phones” section on page 1-8
Restrictions regarding security features	See the “Security Restrictions” section on page 1-13
Viewing a security profile name when running Cisco Unified Communications Manager 5.0 or later	See the “Understanding Security Profiles” section on page 1-12
Identifying phone calls for which security is implemented	See the “Identifying Authenticated, Encrypted, and Protected Phone Calls” section on page 1-12
Transport Layer Security (TLS) connection	See the “Networking Protocols Used with Cisco Unified Wireless IP Phones” section on page 2-9 See the “Phone Configuration Files and Profile Files” section on page 2-14
Security and the phone startup process	See the “Understanding the Phone Startup Process” section on page 3-17
Security and phone configuration files	See the “Phone Configuration Files and Profile Files” section on page 2-14
Changing the TFTP Server 1 or TFTP Server 2 option on the phone when security is implemented	See the “Configuring Network Profiles” section on page 4-8
Items on the Security Configuration menu on the phone	See the “Viewing Security Information” section on page 8-1
Unlocking the CTL file	See the “Accessing the CTL File Screen” section on page 8-3
Disabling access to phone web pages	See the “Specific Configuration Options for the Cisco Unified Wireless IP Phone 7925G” section on page 7-13
Troubleshooting	See the “General Troubleshooting Information” section on page 10-14 Refer to <i>Cisco Unified Communications Manager Security Guide</i> , Troubleshooting chapter
Resetting or restoring the phone	See the “Erasing the Local Configuration” section on page 10-18

Overview of Supported Security Features

Table 1-3 provides an overview of the security features that the Cisco Unified Wireless IP Phone 7925G supports. 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 > System Configuration > Security**. For more information, see the “[Viewing Security Information](#)” section on page 8-1.



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 the *Cisco Unified Communications Manager Security Guide*.

Table 1-3 Description of Security Features

Feature	Description
Image authentication	Prevents tampering with the firmware image before it is loaded on a phone by using signed binary files (with the extension.sbn). Tampering with the image causes a phone to fail the authentication process and reject the new image.
Customer-site certificate installation	Authenticates each Cisco Unified IP Phone by using a unique certificate. Phones include a manufacturing installed certificate (MIC), but for additional security, you can specify in Cisco Unified Communications Manager Administration that a certificate be installed by using the Certificate Authority Proxy Function (CAPF). Alternatively, you can install a locally significant certificate (LSC) from the Security Configuration menu on the phone. See the “ Configuring the Security Certificate on the Phone ” section on page 5-12 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 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.

Table 1-3 Description of Security Features (continued)

Feature	Description
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 Cisco Unified 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.
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 by using TLS	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 non-secure, authenticated, or encrypted. See the “Understanding Security Profiles” section on page 1-12 for more information.
Encrypted configuration files	Lets you ensure the privacy of phone configuration files.
Optional disabling of the web server functionality for a phone	You can prevent access to a phone web page, which displays a variety of operational statistics for the phone.
Phone hardening	Additional security options, which you control from Cisco Unified Communications Manager Administration: <ul style="list-style-type: none"> • Disabling Gratuitous ARP (GARP) • Disabling access to the Setting menus • Disabling access to web pages for a phone <p>Note You can view current settings for the GARP Enabled, and Web Access options by looking at the phone’s Device Information menu. For more information, see the “Viewing Security Information” section on page 8-1.</p>

Related Topics

- [Understanding Security Profiles, page 1-12](#)
- [Identifying Authenticated, Encrypted, and Protected Phone Calls, page 1-12](#)
- [Viewing Device Information, page 8-4](#)
- [Security Restrictions, page 1-13](#)

Understanding Security Profiles

A security profile, which defines whether the phone is non-secure, authenticated, encrypted, or protected is associated with every Cisco Unified IP Phone that is supported by Cisco Unified Communications Manager Administration. For information about configuring the security profile and applying the profile to the phone, refer to *Cisco Unified Communications Manager Security Guide*.

**Note**

For Cisco Unified IP Phones using Cisco Unified CallManager 4.1 and later, security is configured on each phone. For more information about configuring security, refer to *Cisco Unified CallManager Security Guide* at

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.

To view the security mode that is set for the phone, from the phone screen, choose **SETTINGS > Device Information > Security > Security Mode**. For more information, see the “[Viewing Security Information](#)” section on page 8-1.

Related Topics

- [Identifying Authenticated, Encrypted, and Protected Phone Calls, page 1-12](#)
- [Viewing Device Information, page 8-4](#)
- [Security Restrictions, page 1-13](#)

Identifying Authenticated, Encrypted, and Protected Phone Calls

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

In an authenticated call, all devices participating in the establishment of the call are authenticated by 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 screen changes to this icon:



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

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


**Note**

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

Establishing and Identifying Protected Calls

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

A protected call is established using this process:

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

**Note**

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

Related Topics

- [Understanding Security Features for Cisco Unified IP Phones, page 1-8](#)
- [Understanding Security Profiles, page 1-12](#)
- [Security Restrictions, page 1-13](#)

Security Restrictions

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

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

If the phone is configured for encryption, the user 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 non-secure. The authentication icon continues to display on the authenticated phones in the call, even if the initiator's phone does not support security.

Overview of Configuring and Installing the Cisco Unified Wireless IP Phone 7925G

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

After you have set up the IP telephony system and configured system-wide features in Cisco Unified Communications Manager Administration, you can add IP phones to the system. To add wireless IP phones to the IP network, system administrators should conduct a site survey to determine strategic locations for access points (APs) to ensure good wireless voice coverage. For detailed information about a voice over WLAN deployment, refer to the [Cisco Enterprise Mobility 3.0 Design Guide](#).

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

- [Configuring the Cisco Unified Wireless IP Phone 7925G in Cisco Unified Communications Manager, page 1-14](#)
- [Installing the Cisco Unified Wireless IP Phone 7925G, page 1-15](#)

Configuring the Cisco Unified Wireless IP Phone 7925G in Cisco Unified Communications Manager

To add phones to the Cisco Unified Communications Manager Administration, 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 [“Methods for Adding Phones to Cisco Unified Communications Manager” section on page 3-2](#).

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

For a checklist of tasks for configuring the phone in Cisco Unified Communications Manager, see the [“Configuring the Cisco Unified Wireless IP Phone 7925G in Cisco Unified Communications Manager” section on page D-4](#).

Related Topics

- [Installing the Cisco Unified Wireless IP Phone 7925G, page 1-15](#)
- [Configuring Features, Templates, Services, and Users, page 7-1](#)
- [Configuring the Cisco Unified Wireless IP Phone 7925G in Cisco Unified Communications Manager, page D-4](#)

Installing the Cisco Unified Wireless IP Phone 7925G

After you have added the phones to the Cisco Unified Communications Manager Administration, you can complete the phone installation. You or the end users can install the phone at the user location. The Cisco Unified Wireless IP Phone Installation Guide, available online at http://www.cisco.com/en/US/docs/voice_ip_comm/cuipph/7925g/7_0/english/install/guide/7925ig.pdf.html, provides directions for assembling the phone and accessories and charging the battery.

Prior to using the phone to connect to the wireless LAN, you need to configure a network profile for the phone. You can use the phone web pages to set up the network profile and other phone settings, or you can configure the network profile using the menus on the phone.

If you use auto-registration that is part of Cisco Unified Communications Manager Administration, you need to update the specific configuration information for the phone such as associating the phone with a user, changing the softkey template, or directory number (DN).

**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-crypto>.

For a checklist of tasks for installing the phone, see the “[Installing the Cisco Unified Wireless IP Phone 7925G](#)” section on page D-7.

Related Topics

- [Understanding the Cisco Unified Wireless IP Phone 7925G, page 1-1](#)
- [Overview of Configuring and Installing the Cisco Unified Wireless IP Phone 7925G, page 1-14](#)
- [Installing the Cisco Unified Wireless IP Phone 7925G, page D-7](#)
- [Troubleshooting the Cisco Unified Wireless IP Phone 7925G, page 10-1](#)



CHAPTER 2

Overview of the VoIP Wireless Network

This chapter provides an overview of the interaction between the Cisco Unified Wireless IP Phone 7925G and other key components of a VoIP network in a wireless local area network (WLAN) environment. It contains the following sections:

- [Understanding the Wireless LAN, page 2-1](#)
- [Understanding WLAN Standards and Technologies, page 2-3](#)
- [Bluetooth Wireless Technology, page 2-8](#)
- [Components of the VoIP Wireless Network, page 2-9](#)
- [Security for Voice Communications in WLANs, page 2-16](#)
- [VoIP WLAN Configuration, page 2-21](#)
- [Site Survey Verification, page 2-22](#)

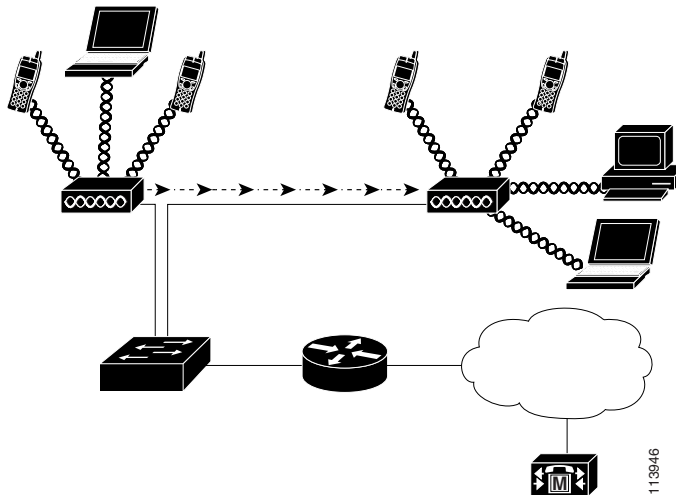
Understanding the Wireless LAN

With the introduction of wireless communication, wireless IP phones can provide voice communication within the corporate WLAN. The Cisco Unified Wireless IP Phone 7925G depends upon and interacts with wireless access points (APs) and key Cisco IP telephony components, including Cisco Unified Communications Manager Administration, to provide wireless voice communication.

In a traditional LAN, IP phones and computers use cables to transmit messages and data packets. Cisco Unified WLAN delivers security, scalability, reliability, ease of deployment, and management similar to wired LANs. It includes RF capabilities that enable real-time access to core business applications and provides proven enterprise-class secure connectivity. The WLAN is an integrated end-to-end solution that uses wireless IP phones and APs, network infrastructure, network management, and mobility services.

[Figure 2-1](#) shows a typical WLAN topology that enables the wireless transmission of voice for wireless IP telephony.

Figure 2-1 WLAN with Wireless IP Phones



When a wireless IP phone powers on, it searches for and becomes associated with an AP. As users move from one location to another, the wireless IP phone roams out-of-range of one AP into the range of another AP. The wireless IP phone builds and maintains a list of eligible APs and reconnects to an AP in that list. See “[Associating to APs](#)” section on page 2-12 for more information.

The AP uses its connection to the wired network to transmit data and voice packets to and from the switches and routers. Voice signaling is transmitted to the Cisco Unified Communications Manager server for call processing and routing.

APs are critical components in a WLAN because they provide the wireless links or “hot spots” to the network. Cisco requires that the APs supporting voice communications use Cisco IOS Release 12.3(8)JA or later. Cisco IOS software provides features for managing voice traffic.

In some WLANs, each AP has a wired connection to an Ethernet switch, such as a Cisco Catalyst 3750, that is configured on a LAN. The switch provides access to gateways and the Cisco Unified Communications Manager server to support wireless IP telephony.

Some networks have wired components that support wireless components. The wired components could consist of switches, routers, and bridges with special modules to enable wireless capability.

The Cisco Unified WLAN can have the following components:

- Cisco Aironet Series Access Points—802.11a/b/g enterprise-class access points with integrated antennas or antenna connections for easy deployment.
- Cisco 2000 Series Wireless LAN Controller—For small to medium sized networks, such as branch offices. Works with Cisco lightweight access points.
- Cisco 4100 Series Wireless LAN Controller—For medium to large deployments. Works with Cisco lightweight access points.
- Cisco 4400 Series Wireless LAN Controller—For large enterprise facilities. The Cisco 4402 and 4404 models support a maximum of 50 and 100 access points respectively.
- Cisco Wireless LAN Controller Module for Integrated Services Routers—Enables small-to-medium businesses and enterprises to deploy and manage secure WLANs at branch offices.
- Cisco Catalyst 6500 Series Wireless Services Module (WiSM)—Provides security, mobility, redundancy, and ease of use for WLAN administrators.

- Cisco Catalyst 3750 Series Integrated Wireless LAN Controllers—Adds wireless LAN controller functions to the stackable Cisco Catalyst 3750G Series Switches to improve operating efficiency, security, mobility, and ease of use for WLAN administrators.
- Wireless Control System (WCS)—Provides a powerful systems management. System administrators can design, control, and monitor enterprise WLANs from a centralized location.
- Cisco 2700 Series Wireless Location Appliance—802.11 based location tracking solution for asset tracking, IT management, and location based security. An open API is included.
- Cisco Wireless LAN Client Adapters—Available in CardBus, PCMCIA and PCI form factors, Cisco Aironet Wireless LAN Client Adapters connect desktop and mobile computing devices to the WLAN in 802.11b-compliant or 802.11a-compliant network.

For more information about Cisco Unified Wireless Networks, refer to <http://www.cisco.com/en/US/products/hw/wireless/index.html>

Understanding WLAN Standards and Technologies

This section describes the following concepts:

- [802.11 Standards for WLAN Communications, page 2-3](#)
- [Radio Frequency Ranges, page 2-4](#)
- [802.11 Data Rates, Tx Power, Ranges, and Decibel Tolerances, page 2-4](#)
- [Wireless Modulation Technologies, page 2-5](#)
- [AP, Channel, and Domain Relationships, page 2-6](#)
- [WLANs and Roaming, page 2-7](#)

802.11 Standards for WLAN Communications

Wireless LANs must follow the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standards that define the protocols that govern all Ethernet-based wireless traffic. The Cisco Unified Wireless IP Phone 7925G supports the following standards:

- 802.11b—Specifies the radio frequency (RF) of 2.4 GHz for both transmitting and receiving data. Commonly called the Wi-Fi standard.
- 802.11g—Uses the same unlicensed 2.4 GHz band as 802.11b, but extends the data rates to provide greater performance by using Orthogonal Frequency Division Multiplexing (OFDM) technology. OFDM is a physical-layer encoding technology for transmitting signals by using RF.
- 802.11a—Uses the 5 GHz band that provides more channels and improved data rates by using OFDM technology. Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) supports this standard.
- 802.11d—Enables APs to communicate available radio channels and acceptable power levels. The Cisco Unified Wireless IP Phone 7925G will always give precedence to 802.11d to determine which channels and powers to use. If the information is unavailable, then the phone will fallback to the locally configured regulatory domain.

Radio Frequency Ranges

WLAN communications use the following RF ranges:

- 2.4 GHz—Does not require licensing. To reduce interference within this bandwidth, WLANs transmit on non-overlapping channels, which are typically limited to three channels, although Japan uses four channels.
Many devices operate in the 2.4 GHz bandwidth including cordless phones and microwave ovens and can interfere with wireless communications. Interference does not destroy the signal, but can reduce the transmission speed from 11 Mbps to 1 Mbps. RF interference can affect voice quality over the wireless network.
- 5 GHz—Divided into several sections called Unlicensed National Information Infrastructure (UNII) bands and has four channels each. The channels are spaced at 20 MHz to provide non-overlapping channels and more channels than 802.11b or 802.11g.

Table 2-1 lists frequency band ranges and operating channels by regulatory domain.

Table 2-1 Frequency Bands and Operating Channels by Regulatory Domain

Regulatory Domain	Frequency Band Range	Operating Channels
Federal Communications Commission (FCC)	2.412-2.462 GHz	11 channels
Product number is CP-7925GA-K9	5.15-5.25 GHz (UNII-1) 5.25-5.35 GHz (UNII-2) 5.725-5.825 (UNII-3) 5.470 - 5.725 (DFS) 5.47-5.725 GHz (pending approval)	8 of 11 channels 11 channels
ETSI (Europe)	2.412-2.472 GHz	13 channels
Product number is CP-7925GE-K9	5.15-5.725 GHz	19 channels
Japan	2.412-2.472 GHz	13 channels (ODFM)
Product number is CP-7925GPC-CH1-K9	2.412-2.484 GHz 5.15-5.35 GHz	14 channels (CCK) 8 channels
World Product number is CP-7925GW-K9	—	Uses 802.11d to identify band ranges and channels

802.11 Data Rates, Tx Power, Ranges, and Decibel Tolerances

Table 2-2 lists the Tx power capacities, data rates, ranges in feet and meters, and decibels tolerated by the receiver by 801.11 standard.

Table 2-2 Tx Power, Data Rates, Ranges, and Decibels by Standard

Standard	Maximum Tx Power ¹	Data Rate ²	Range	Receiver Sensitivity
802.11a				
	40mW	6 Mbps	610 ft (186 m)	-89 dBm
		9 Mbps	610 ft (186 m)	-88 dBm
		12 Mbps	558 ft (170 m)	-86 dBm
		18 Mbps	541 ft (165 m)	-85 dBm
		24 Mbps	508 ft (155 m)	-82 dBm
		36 Mbps	426 ft (130 m)	-80 dBm
		48 Mbps	328 ft (100 m)	-76 dBm
		54 Mbps	295 ft (90 m)	-74 dBm
802.11g				
	40mW	6 Mbps	722 ft (220 m)	-90 dBm
		9 Mbps	656 ft (200 m)	-89 dBm
		12 Mbps	623 ft (190 m)	-87 dBm
		18 Mbps	623 ft (190 m)	-85 dBm
		24 Mbps	623 ft (190 m)	-82 dBm
		36 Mbps	492 ft (150 m)	-78 dBm
		48 Mbps	410 ft (125 m)	-74 dBm
		54 Mbps	394 ft (120 m)	-73 dBm
802.11b				
	50mW	1 Mbps	1,027 ft (313 m)	-95 dBm
		2 Mbps	951 ft (290 m)	-89 dBm
		5.5 Mbps	853 ft (260 m)	-89 dBm
		11 Mbps	787 ft (240 m)	-85 dBm

1. Adjusts dynamically when associating with an AP if the AP client setting is enabled.
2. Advertised rates by the APs are used. If the Restricted Data Rates functionality is enabled in the Cisco Unified Communications Manager Administration phone configuration, then the Traffic Stream Rate Set IE (CCX V4) is used.

Wireless Modulation Technologies

Wireless communications uses the following modulation technologies for signaling:

- Direct-Sequence Spread Spectrum (DSSS)—Prevents interference by spreading the signal over the frequency range or bandwidth. DSSS technology multiplexes chunks of data over several frequencies so that multiple devices can communicate without interference. Each device has a special code that identifies its data packets and all others are ignored. Cisco wireless 802.11b/g products use DSSS technology to support multiple devices on the WLAN.

- Orthogonal Frequency Division Multiplexing (OFDM)—Transmits signals by using RF. OFDM is a physical-layer encoding technology that breaks one high-speed data carrier into several lower-speed carriers to transmit in parallel across the RF spectrum. OFDM, when used with 802.11g and 802.11a, can support data rates as high as 54 Mbps.

Table 2-3 provides a comparison of data rates, number of channels, and modulation technologies by standard.

Table 2-3 Data Rates, Number of Channels, and Modulation Technologies by IEEE Standard

Item	802.11b	802.11g	802.11a
Data Rates	1, 2, 5.5, 11 Mbps	6, 9, 12, 18, 24, 36, 48, 54 Mbps	6, 9, 12, 18, 24, 36, 48, 54 Mbps
Non-overlapping Channels	3 (Japan uses 4)	3 (Japan uses 4)	Up to 23
Wireless Modulation	DSSS	DSSS, OFDM	OFDM

AP, Channel, and Domain Relationships

APs transmit and receive RF signals over channels within the 2.4 GHz or 5.1 to 5.8 GHz frequency band. To provide a stable wireless environment and reduce channel interference, you must specify non-overlapping channels for each AP. The recommended channels for 802.11b and 802.11g in North America are 1, 6, and 11.

Regulatory domains determine the number of channels that wireless communications can use within the frequency band. Table 2-1 lists the frequency ranges, operating channels, and product numbers for four regulatory domains. The Cisco Unified Wireless IP Phone 7925G uses the fourth domain for all other regions in the world. Wireless LANs in the rest of the world use 802.11d to identify band ranges and channels.



Note

In a non controller-based wireless network, it is recommended that you statically configure channels for each AP. If your wireless network uses a controller, use the Auto-RF feature with minimal voice disruption.

The AP coverage area depends on its type of antenna and transmission power. The AP coverage range is from 500 to 1000 feet with effective isotropic radiated power (EIRP) output that scales at 1, 5, 20, and 50 mW. To provide effective coverage, APs need a range overlap of approximately 20 percent to allow uninterrupted connections as phone users roam from one AP to another.

Wireless networks use a service set identifier (SSID). The SSID differentiates one WLAN from another, so all APs and all devices attempting to connect to a specific WLAN must use the same SSID. The SSID groups user devices and associates the group with the APs.

For more information about wireless network components and design, refer to the *Overview: Cisco Unified Wireless Network* at http://www.cisco.com/en/US/solutions/ns175/networking_solutions_products_genericcontent0900aecd80529a5f.html.

For more information about APs, see the “VoIP WLAN Configuration” section on page 2-21.

WLANs and Roaming

Wireless IP phones provide communication mobility to users within the WLAN environment. Unlike cellular phones that have broad coverage, the coverage area for the wireless IP phone is smaller; therefore, phone users frequently roam from one AP to another. To understand some of the limitations of roaming with wireless IP phones, these examples provide information about the WLAN environment.

- **Pre-call Roaming**—A wireless IP phone user powers on the phone in the office, and the phone associates with the nearby AP. The user leaves the building, moves to another building, and then places a call. The phone associates with a different AP in order to place the call from the new location. If the associated AP is within the same Layer 2 VLAN, the IP address remains the same for the phone. But, if the roaming phone crosses a Layer 3 boundary with DHCP enabled, the phone recognizes that it is no longer in the same subnet. The phone requests a new IP address before it can connect to the network and place the call.



Note If a user leaves the WLAN coverage area and then comes back into the *same* WLAN area, the phone must reconnect to the network. By pressing a key on the phone, the user activates the phone and increases the scanning rate to speed up reconnecting to the network.

- **Mid-call Roaming**—A wireless IP phone user is actively engaged in a call and moves from one building to another. The roaming event occurs when the phone moves into the range of a different AP, and then the phone authenticates and associates with the new AP. The previous AP hands the call over to the new AP while maintaining continuous audio connection without user intervention. As long as the APs are in the same Layer 2 subnet, the wireless IP phone keeps the same IP address and the call continues. As a wireless IP phone roams between APs, it must re-authenticate with each new AP. See the “[Authentication Methods](#)” section on page 2-16 for information about authentication.

If the wireless IP phone user moves from an AP that covers IP Subnet A to an AP that covers IP Subnet B, the phone no longer has an IP address or gateway that is valid within the new subnet and the call can disconnect.

- **Layer 3 Roaming**—With the release of the Cisco Catalyst 6500 Series Wireless LAN Services Module (WLSM), the Cisco Unified Wireless IP Phone 7925G now supports Layer 3 roaming for autonomous mode APs. For details about the Cisco WLSM, refer to the product documentation available at:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/wlsm_1_1/index.htm

Layer 3 roaming with lightweight mode APs is accomplished by controllers that use dynamic interface tunneling. Clients that roam across controllers and VLANS can keep their IP address when using the same SSID.

- **Fast and Secure Roaming**—Cisco Centralized Key Management (CCKM) enables authenticated client devices to roam securely from one AP to another without any perceptible delay during reassociation. With the support of CCKM protocol, the wireless IP phone is able to negotiate the handoff from one AP to another more easily. During the roaming process, the phone must scan for the nearby APs, determine which AP can provide the best service, and then reassociate with the new AP. When implementing stronger authentication methods, such as WPA and EAP, the number of information exchanges increases and causes more delay during roaming. To avoid additional delays, use CCKM to manage authentication.

CCKM, a centralized key management protocol, provides a cache of session credentials on the wireless domain server (WDS). As the phone roams from one AP to the next, CCKM compresses the number of message exchanges during roaming by providing a master key stored on the WDS for the AP to use. The reassociation exchange is reduced to two messages, thereby reducing the roaming time.

For details about CCKM, refer to the “Cisco Fast Secure Roaming Application Note” at: http://www.cisco.com/en/US/products/hw/wireless/ps4570/prod_technical_reference09186a00801c5223.html

**Note**

In dual band WLANs, it is possible to roam between 2.4 GHz bands (802.11b/g) and 5 GHz bands (802.11a). The phone moves out of range of one AP using one band and into the range of another that has the same SSID but is using a different band. This can cause gaps in voice communications. To avoid these communication gaps, try to use only one band for voice communications.

Related Topics

- [Voice QoS in a Wireless Network, page 2-12](#)
- [Configuring the Wireless Network for Voice, page 2-22](#)
- [VoIP WLAN Configuration, page 2-21](#)

Bluetooth Wireless Technology

Bluetooth Class 2.0 with Extended Data Rate (EDR) is a short-range wireless technology that is supported by the Cisco Unified Wireless IP Phone 7925G. It supports the Hands-Free Profile version 1.5.

Your Cisco Unified Wireless IP Phone 7925G is a qualified Bluetooth wireless device (Qualified Device ID (QDID) B014396) and provides voice communication over the same wireless LAN that your computer uses.

Bluetooth enables low bandwidth wireless connections within a range of 10 meters. The best performance is in the 1 to 2 meter range. Synchronous voice channels are provided by using circuit switching and asynchronous data channels are provided by using packet switching.

Bluetooth wireless technology operates in the 2.4 GHz band which is the same as the 802.11b/g band. There can be a potential interference issues. It is recommended that you:

- Use 802.11a that operates in the 5 GHz band.
- Reduce the proximity of other 802.11b/g devices, Bluetooth devices, microwave ovens, and large metal objects.
- Use the Cisco Unified Wireless IP Phone 7925G on the same side of the body as the Bluetooth-enabled headset.

Pairing Headsets

The Cisco Unified Wireless IP Phone 7925G pairs with headsets using a shared key authentication and encryption method. The authentication process can require a personal identification number (PIN) specific to the headset, commonly “0000.” The Cisco Unified Wireless IP Phone 7925G can be paired with more than one headset at a time. Pairing is typically performed once for each headset.

Once a device has been paired, its Bluetooth connection is maintained as long as both devices (phone and headset) are enabled and within range of each other. The connection re-establishes itself automatically if either of the devices powers down then powers up. The green-dotted Bluetooth icon indicates whether or not a device is connected.

When headsets are more than 10 meters away from Cisco Unified Wireless IP Phone 7925G, Bluetooth drops the connection after a 15 to 20 second timeout. If the paired headset comes back into range of the Cisco Unified Wireless IP Phone 7925G and the phone is not connected to another Bluetooth headset, then the in-range Bluetooth headset automatically reconnects. For certain phone types that operate in power-save modes, the user may have to “wake-up” the headset by tapping on its operational button to initiate the reconnect.

**Note**

It is recommended that users read the headset user guide for more information about pairing and connecting the headsets.

Components of the VoIP Wireless Network

The wireless IP phone must interact with several network components in the WLAN to successfully place and receive calls. The following topics describe network components:

- [Networking Protocols Used with Cisco Unified Wireless IP Phones, page 2-9](#)
- [Interacting with Cisco Unified Wireless APs, page 2-11](#)
- [Voice QoS in a Wireless Network, page 2-12](#)
- [Interacting with Cisco Unified Communications Manager, page 2-14](#)
- [Interacting with the Dynamic Host Configuration Protocol Server, page 2-15](#)

Networking Protocols Used with Cisco Unified Wireless IP Phones

Cisco Unified IP Phones support several networking protocols for voice communication. [Table 2-4](#) describes the networking protocols that the Cisco Unified Wireless IP Phone 7925G supports.

Table 2-4 Supported Networking Protocols

Networking Protocol	Purpose	Usage Notes
Cisco Discovery Protocol (CDP)	<p>Device-discovery protocol that runs on all Cisco-manufactured equipment.</p> <p>Using CDP, a device can advertise its existence to other devices and receive information about other devices in the network.</p>	Cisco Unified IP Phones use CDP to communicate information such as auxiliary VLAN ID, per-port power management details, and QoS configuration information with the Cisco Catalyst switch.
Dynamic Host Configuration Protocol (DHCP)	<p>Dynamically allocates and assigns an IP address to network devices.</p> <p>DHCP enables an IP phone to connect to the network and become operational without the administrator assigning an IP address or configuring additional network parameters.</p>	<p>DHCP is enabled by default. If disabled, you must manually configure the IP address, subnet mask, gateway, and an TFTP server on each phone locally.</p> <p>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 to <i>Cisco Unified Communications Manager System Guide</i>.</p>
IP	Messaging protocol that addresses and sends packets across the network.	<p>To communicate using IP, network devices must have an assigned IP address, subnet, and gateway.</p> <p>IP addresses, subnet, and gateway identifications are automatically assigned if you are using the Cisco Unified IP Phone with DHCP. If you are not using DHCP, you must manually assign these properties to each phone locally.</p>
Real-Time Control Protocol (RTCP)	Used with the RTP protocol to provide control over the transporting of real-time data, such as interactive voice and video, over data networks.	Cisco Unified IP Phones use the RTCP protocol to allow monitoring of the data delivery and minimal control and identification functionality.
RTP	Standard 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.
SCCP	Uses Cisco-proprietary messages to communicate between IP devices and Cisco Unified Communications Manager, Release 4.x, 5.1, 6.0, 6.1, and 7.0.	Cisco Unified IP Phones use SCCP protocol for VoIP call signaling and enhanced features such as Message Waiting Indication (MWI).

Table 2-4 Supported Networking Protocols (continued)

Networking Protocol	Purpose	Usage Notes
TCP	Connection-oriented transport protocol.	Cisco Unified IP Phones use TCP to connect to Cisco Unified Communications Manager and to access XML services.
TFTP	Method for transferring files over the network. On the Cisco Unified IP Phone, TFTP enables you to obtain a configuration file specific to the phone type.	You must have a TFTP server in your network that the DHCP server automatically identifies. If more than one TFTP server is running in your network, you must manually assign a TFTP server to each phone.
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.
User Datagram Protocol (UDP)	Connectionless messaging protocol for delivery of data packets.	Cisco Unified IP Phones receive and process UDP messages. RTP voice traffic runs over UDP.

Related Topics

- [Understanding the Phone Startup Process, page 3-17](#)
- [Components of the VoIP Wireless Network, page 2-9](#)
- [Configuring DHCP Settings, page 5-6](#)

Interacting with Cisco Unified Wireless APs

Wireless IP phones use the same APs as wireless data devices. However, voice traffic over a WLAN requires different equipment configurations and layouts than a WLAN that is used exclusively for data traffic. Data transmission can tolerate a higher level of RF noise, packet loss, and channel contention than voice transmission. Packet loss during voice transmission can cause choppy or broken audio and make the phone call inaudible.

Wireless IP Phones users are mobile and often roam across a campus or between floors in a building while connected to a call. In contrast, data users remain in one place or occasionally move to another location. The ability to roam while maintaining a call is one of the advantages of wireless voice so RF coverage needs to include stairwells, elevators, quiet corners outside conference rooms, and passage ways.

To ensure good voice quality and optimal RF signal coverage, you must perform a site survey. The site survey will determine settings suitable to wireless voice and assist in the design and layout of the WLAN; for example AP placement, power levels, and channel assignments.

After deploying and using wireless voice, you should continue to perform post installation site surveys. When you add a group of new users, install more equipment, or stack large amounts of inventory, you are changing the wireless environment. A post installation survey will verify that the AP coverage is still adequate for optimal voice communications. See the [“Site Survey Verification” section on page 2-22](#) for more information.

Associating to APs

At startup, the Cisco Unified Wireless IP Phone 7925G scans for APs with SSIDs and encryption types that it recognizes. The phone builds and maintains a list of eligible APs and uses the following variables to determine the best AP.

- Received Signal Strength Indicator (RSSI)—Signal strength of available APs within the RF coverage area. The phone attempts to associate with the AP with the highest RSSI value.
- QoS Basic Service Set (QBSS)—Beacon information element (IE) that sends the channel usage of the AP to the wireless IP phone. The phone uses the QBSS value to determine whether the AP can effectively handle more traffic.



Note QBSS is not supported when using Wi-Fi 802.11a.

- Traffic Specification (TSpec)—Calculation of call limits and WLAN load balancing. The TSpec value of each voice stream allows the system to allocate bandwidth to voice devices on a first-come, first-served basis. For more information, see [“Voice QoS in a Wireless Network” section on page 2-12](#).

The wireless IP phone associates with the AP with the highest RSSI and lowest channel usage values (QBSS) that have matching SSID and encryption types. To ensure that voice traffic is handled properly, you must configure the correct QoS in the AP. For configuration information, see [“Wireless Network Requirements for VoIP” section on page 2-21](#).

Related Topics

- [Security for Voice Communications in WLANs, page 2-16](#)
- [VoIP WLAN Configuration, page 2-21](#)

Voice QoS in a Wireless Network

Voice traffic on the Wireless LAN, like data traffic, is susceptible to delay, jitter, and packet loss. These issues do not impact the data end user, but have serious implications for a voice call. To ensure that voice traffic receives timely and reliable treatment with low delay and low jitter, you must use Quality of Service (QoS), and use separate virtual LANs (VLANs) for voice and data. By isolating the voice traffic onto a separate VLAN, you can use QoS to provide priority treatment for voice packets when traveling across the network. Also, use a separate VLAN for data traffic, not the default native VLAN which is typically used for all network devices.

You need the following VLANs on the network switches and the APs that support voice connections on the WLAN.

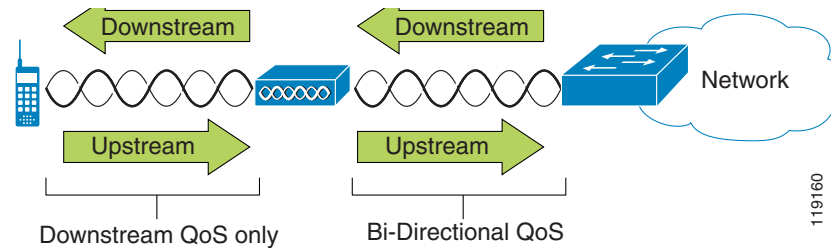
- Voice VLAN—Voice traffic to and from the wireless IP phone
- Data VLAN—Data traffic to and from the wireless PC
- Native VLAN—Data traffic to and from other wireless devices

Assign separate SSIDs to the voice and to the data VLANs. If you configure a separate management VLAN in the WLAN, do not associate an SSID with the management VLAN.

By separating the phones into a voice VLAN and marking voice packets with higher QoS, you can ensure that voice traffic gets priority treatment over data traffic resulting in lower packet delay and fewer lost packets.

Unlike wired networks with dedicated bandwidths, wireless LANs consider traffic direction when implementing QoS. Traffic is classified as upstream or downstream from the point of view of the AP as shown in Figure 2-2.

Figure 2-2 Voice Traffic in a Wireless Network



Beginning with Cisco IOS release 12.2(11)JA, Cisco Aironet APs support the contention-based channel access mechanism called Enhanced Distributed Coordination Function (EDCF). The EDCF-type of QoS has up to eight queues for downstream (toward the 802.11b/g clients) QoS. You can allocate the queues based on these options:

- QoS or Differentiated Services Code Point (DSCP) settings for the packets
- Layer 2 or Layer 3 access lists
- VLANs for specific traffic
- Dynamic registration of devices

Although you can have up to eight queues on the AP, you should use only two queues for voice traffic to ensure the best possible voice QoS. Place voice (RTP) and signaling (SCCP) traffic in the highest priority queue, and place data traffic in a best-effort queue. Although 802.11b/g EDCF does not guarantee that voice traffic is protected from data traffic, you should get the best statistical results by using this queuing model.



Note The Cisco Unified Wireless IP Phone 7925G marks the SCCP signaling packets with a DSCP value of 24 and RTP packets with DSCP value of 46.

To improve reliability of voice transmissions in a nondeterministic environment, the Cisco Unified Wireless IP Phone 7925G supports the IEEE 802.11e industry standard and is Wi-Fi Multimedia (WMM) capable. WMM enables differentiated services for voice, video, best effort data and other traffic. However, in order for these differentiated services to provide sufficient QoS for voice packets, only a certain amount of voice bandwidth can be serviced or admitted on a channel at one time. If the network can handle “N” voice calls with reserved bandwidth, when the amount of voice traffic is increased beyond this limit, (to N+1 calls), the quality of all calls suffers.

To help address the problems of VoIP stability and roaming, an initial Call Admission Control (CAC) scheme is required. With CAC, QoS is maintained in a network overload scenario by ensuring that the number of active voice calls does not exceed the configured limits on the AP. The Cisco Unified Wireless IP Phone 7925G can integrate layer 2 TSpec admission control with layer 3 Cisco Unified Communications Manager admission control (RSVP). During times of network congestion, calling or called parties receive a fast busy indication. The system maintains a small bandwidth reserve so wireless phone clients can roam into a neighboring AP (AP), even when the AP is at “full capacity”. After reaching the voice bandwidth limit, the next call is load-balanced to a neighboring AP without affecting the quality of the existing calls on the channel.

Implementing QoS in the connected Ethernet switch is highly desirable to maintain good voice quality. The COS and DSCP values that the Cisco Unified Wireless IP Phone 7925G sets do not need to be modified. To configure QoS correctly on the AP, see the [“Wireless Network Requirements for VoIP” section on page 2-21](#).

Related Topics

- [Authentication Methods, page 2-16](#)
- [Interacting with Cisco Unified Communications Manager, page 2-14](#)
- [VoIP WLAN Configuration, page 2-21](#)

Interacting with Cisco Unified Communications Manager

Cisco Unified Communications Manager is the call control component in the network that handles and routes calls for the wireless IP phones. Cisco Unified Communications Manager manages the components of the IP telephony system—the phones, access gateways, and the resources—for such features as call conferencing and route planning. When deploying Cisco Unified Wireless IP Phone 7925G, you must use Cisco Unified Communications Manager Release 4.1, 4.2, 4.3, 5.1, 6.0(1), 6.1(1) or 7.0(1) and SCCP protocol.

Before Cisco Unified Communications Manager can recognize a phone, it must register with Cisco Unified Communications Manager and be configured in the database. For information about setting up phones in Cisco Unified Communications Manager, see the [“Overview of Configuring and Installing the Cisco Unified Wireless IP Phone 7925G” section on page 1-14](#).

You can find more information about configuring Cisco Unified Communications Manager to work with the IP phones and IP devices in the *Cisco Unified Communications Manager Administration Guide* and *Cisco Unified Communications Manager System Guide*.

Related Topics

- [Overview of Configuring and Installing the Cisco Unified Wireless IP Phone 7925G, page 1-14](#)
- [Phone Configuration Files and Profile Files, page 2-14](#)

Phone Configuration Files and Profile Files

Configuration files for a phone define parameters for connecting to Cisco Unified Communications Manager and are stored on the TFTP server. In general, any time you make a change in Cisco Unified Communications Manager Administration that requires resetting the phone, the phone configuration file changes automatically.

Configuration files also contain information about the correct image load for the phone. If this image load differs from the one currently loaded on a phone, the phone contacts the TFTP server to request the new image file.

The phone first requests the configuration file `SEPxxxxxxxxxxx.cnf.xml`, where each `xx` is the two-digit lowercase hexadecimal representation of each integer in the MAC address. If the phone cannot find this file, it requests the configuration file `XMLDefault.cnf.xml`.

After the phone obtains the `*.cnf.xml` files, it requests a phone-specific profile file. If a phone cannot find this profile file, it requests the appropriate common profile file.

After the phone finds one of the profile files, or if it cannot find a profile file, it continues with its startup process.

Related Topic

[Understanding the Phone Startup Process, page 3-17](#)

Interacting with the Dynamic Host Configuration Protocol Server

Dynamic Host Configuration Protocol (DHCP) is a communications protocol that lets network administrators manage and automate the assignment of IP addresses in a network. When an IP device is added to the network, it must have a unique IP address. Without DHCP, the IP address must be entered manually at each device. DHCP allocates IP addresses dynamically and reuses IP addresses when devices no longer need them.

If DHCP is enabled in the network, the Cisco Unified Wireless IP Phone 7925G uses the DHCP scope settings in the DHCP server to perform the phone provisioning bootup process. You must configure the settings of the DHCP server in the Cisco Unified Communications Manager network.

The DHCP scope settings include the following:

- TFTP servers
- DNS server IP address (optional unless using host names)
- Pool and range of the subnet mask, IP address, and gateway

The priority of the DHCP settings for the TFTP server is unique to the Cisco Unified Wireless IP Phone 7925G, as shown in [Table 2-5](#).

Table 2-5 *DHCP Settings Priority*

Priority	DHCP Settings
1st	DHCP option 150
2nd	DHCP option 66
3rd	SIADDR
4th	ciscoCM1

If DHCP is disabled, the Cisco Unified Wireless IP Phone 7925G uses the following network settings in [Table 2-6](#) to perform the phone provisioning bootup process. You must configure these static parameters for each Cisco Unified Wireless IP Phone 7925G.

Table 2-6 *Static IP Addresses When DHCP is Disabled*

Static Setting	Description
IP Address	IP address, the unique identifier assigned by the system administrator for the phone.
Subnet Mask	Used to partition the IP address into a network identifier and host identifier so TCP/IP can distinguish between them.
Default Router 1	Identifies the gateway that provides connectivity to the IP network beyond the subnet to which the phone belongs.

Table 2-6 *Static IP Addresses When DHCP is Disabled (continued)*

Static Setting	Description
DNS Server 1 DNS Server 2	If the system is configured to use host names for servers instead of IP addresses, identifies the primary and secondary DNS server to resolve host names.
TFTP Server 1 TFTP Server 2	Identifies the TFTP servers that the phone uses to obtain configuration files.

Security for Voice Communications in WLANs

Because all WLAN devices that are within range can receive all other WLAN traffic, securing voice communications is critical in WLANs. To ensure that voice traffic is not manipulated or intercepted by intruders, the Cisco Unified Wireless IP Phone 7925G and Cisco Aironet APs are supported in the Cisco SAFE Security architecture. For more information about security in networks, refer to http://www.cisco.com/en/US/netsol/ns744/networking_solutions_program_home.html.

This section contains the following items:

- [Authentication Methods, page 2-16](#)
- [Authenticated Key Management, page 2-18](#)
- [Encryption Methods, page 2-18](#)
- [Choosing AP Authentication and Encryption Methods, page 2-18](#)

Authentication Methods

The Cisco Wireless IP telephony solution provides wireless network security that prevents unauthorized logins and compromised communications by using the following authentication methods.

- **Open Authentication**—Any wireless device can request authentication in an open system. The AP that receives the request may grant authentication to any requestor or only to requestors on a list of users. Communication between the wireless device and AP could be non-encrypted or devices can use Wired Equivalent Privacy (WEP) keys to provide security. Devices that are using WEP only attempt to authenticate with an AP that is using WEP.
- **Shared Key Authentication**—The AP sends an unencrypted challenge text string to any device attempting to communicate with the AP. The device that is requesting authentication uses a pre-configured WEP key to encrypt the challenge text and sends it back to the AP. If the challenge text is encrypted correctly, the AP allows the requesting device to authenticate. A device can authenticate only if its WEP key matches the WEP key on the APs.

Shared key authentication can be less secure than open authentication with WEP because someone can monitor the challenges. An intruder can calculate the WEP key by comparing the unencrypted and encrypted challenge text strings.

- **Wireless Protected Access (WPA) Pre-Shared Key (PSK) Authentication**—The AP and the phone are configured with the same authentication key. The pre-shared key is used to create unique pair-wise keys that are exchanged between each phone and the AP. You can configure the pre-shared key as a hexadecimal or ASCII character string. Because the pre-shared key is stored on the phone, it might be compromised if the phone is lost or stolen.

- **Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) Authentication**—This client server security architecture encrypts EAP transactions within a Transport Level Security (TLS) tunnel between the AP and the RADIUS server such as the Cisco Access Control Server (ACS).

The TLS tunnel uses Protected Access Credentials (PACs) for authentication between the client (phone) and the RADIUS server. The server sends an Authority ID (AID) to the client (phone), which in turn selects the appropriate PAC. The client (phone) returns a PAC-Opaque to the RADIUS server. The server decrypts the PAC with its master-key. Both end points now have the PAC key and a TLS tunnel is created. EAP-FAST supports automatic PAC provisioning, but you must enable it on the RADIUS server.

**Note**

In the Cisco ACS, by default, the PAC expires in one week. If the phone has an expired PAC, authentication with the RADIUS server takes longer while the phone gets a new PAC. To avoid the PAC provisioning delays, set the PAC expiration period to 90 days or longer on the ACS or RADIUS server.

- **Extended Authentication Protocol Transport Level Security (EAP-TLS) Authentication**—EAP-TLS/RFC 2716 uses the TLS protocol (RFC 2246), which is the latest IETF version of the SSL security protocol. TLS provides a way to use certificates for both user and server authentication, and for dynamic session key generation.

Microsoft Windows XP provides support for 802.1x, allowing EAP authentication protocols (including EAP-TLS) to be used for authentication. The authentication used in EAP-TLS is mutual: the server authenticates the user and the user authenticates the server. Mutual authentication is required in a WLAN. EAP-TLS provides excellent security but requires client certificate management.

EAP-TLS uses Public Key Infrastructure (PKI) with the following conditions:

- Wireless LAN client (user machine) requires a valid certificate to authenticate to the WLAN network.
 - AAA server requires a “server” certificate to validate its identity to the clients.
 - Certificate Authority (CA) server infrastructure issues certificates to the AAA server and the clients.
- **Protected Extensible Authentication Protocol (PEAP) Authentication**—PEAP uses server-side public key certificates to authenticate clients by creating an encrypted SSL/TLS tunnel between the client and the authentication server.
 - **PEAP with Server Certificate Authentication**—The Cisco Unified Wireless IP Phone 7925G can validate the server certificate during the authentication handshakes over an 802.11 wireless link. This functionality is disabled by default and is enabled in Cisco Unified Communications Manager Administration.

The exchange of authentication information is encrypted and the user credentials are safe from eavesdropping. MS-CHAP v2 is the supported inner authentication protocol.

- **Light Extensible Authentication Protocol (LEAP)**—Cisco proprietary password-based mutual authentication scheme between the client (phone) and a RADIUS server. Cisco Unified Wireless IP Phone 7925G can use LEAP for authentication with the wireless network.

This section describes the following concepts:

- [Authenticated Key Management, page 2-18](#)
- [Encryption Methods, page 2-18](#)

Authenticated Key Management

The following authentication schemes use the RADIUS server to manage authentication keys:

- WPA—Uses information on a RADIUS server to generate unique keys for authentication. Because these keys are generated at the centralized RADIUS server, WPA provides more security than WPA pre-shared keys that are stored on the AP and phone.
- Cisco Centralized Key Management (CCKM)—Uses information on a RADIUS server and a wireless domain server (WDS) to manage and authenticate keys. The WDS creates a cache of security credentials for CCKM-enabled client devices for fast and secure reauthentication.

With WPA and CCKM, encryption keys are not entered on the phone, but are automatically derived between the AP and phone. But the EAP username and password that are used for authentication must be entered on each phone.

Encryption Methods

To ensure that voice traffic is secure, the Cisco Unified Wireless IP Phone 7925G supports WEP, TKIP, and Advanced Encryption Standards (AES) for encryption. When using these mechanisms for encryption, both the signaling Skinny Client Control Protocol (SCCP) packets and voice Real-Time Transport Protocol (RTP) packets are encrypted between the AP and the wireless IP phone.

- WEP—When using WEP in the wireless network, authentication happens at the AP by using open or shared-key authentication. The WEP key that is setup on the phone must match the WEP key that is configured at the AP for successful connections. The Cisco Unified Wireless IP Phone 7925G supports WEP keys that use 40-bit encryption or a 128-bit encryption and remain static on the phone and AP.

EAP and CCKM authentication can use WEP keys for encryption. The RADIUS server manages the WEP key and passes a unique key to the AP after authentication for encrypting all voice packets; consequently, these WEP keys can change with each authentication.

- TKIP—WPA and CCKM use TKIP encryption that has several improvements over WEP. TKIP provides per-packet key ciphering and longer initialization vectors (IVs) that strengthen encryption. In addition, a message integrity check (MIC) ensures that encrypted packets are not being altered. TKIP removes the predictability of WEP that helps intruders decipher the WEP key.
- AES—An encryption method used for WPA2 authentication. This national standard for encryption uses a symmetrical algorithm that has the same key for encryption and decryption. AES uses Cipher Blocking Chain (CBC) encryption of 128 bits in size, supporting key sizes of 128, 192 and 256 bits, as a minimum.



Note The Cisco Unified Wireless IP Phone 7925G does not support Cisco Key Integrity Protocol (CKIP) with CMIC.

Choosing AP Authentication and Encryption Methods

Authentication and encryption schemes are setup within the wireless LAN. VLANs are configured in the network and on the APs and specify different combinations of authentication and encryption. An SSID is associated with a VLAN and its particular authentication and encryption scheme. In order for wireless client devices to authenticate successfully, you must configure the same SSIDs with their authentication and encryption schemes on the APs and on the wireless IP phone.

Some authentication schemes require specific types of encryption. With Open authentication, you have the option to use static WEP for encryption for added security. But if you are using Shared Key authentication, you must set static WEP for encryption, and you must configure a WEP key on the phone.

When using Authenticated Key Management (AKM) for the Cisco Unified Wireless IP Phone 7925G, several choices for both authentication and encryption can be set up on the APs with different SSIDs. When the phone attempts to authenticate, it chooses the AP that advertises the authentication and encryption scheme that the phone can support. Auto (AKM) mode can authenticate by using WPA, WPA2, WPA Pre-shared key, or CCKM.

**Note**

- When using WPA Pre-shared key or WPA2 Pre-shared key, the pre-shared key must be statically set on the phone. These keys must match the keys configured on the AP.
- When using Auto (AKM), encryption options are automatically configured for WPA, WPA2, WPA Pre-shared key, WPA2 Pre-shared key, or CCKM.
- In AKM mode, the phone will authenticate with LEAP if it is configured with WPA, WPA2, or CCKM key management.
- The Cisco Unified Wireless IP Phone 7925G does not support auto EAP negotiation; to use EAP-FAST mode, you must specify it.
- If AKM and 802.1x are used, the authentication method is LEAP.
- The Cisco Unified Wireless IP Phone 7925G uses network EAP for 802.1x but you can enable open EAP.

Table 2-7 provides a list of authentication and encryption schemes configured on the Cisco Aironet APs supported by the Cisco Unified Wireless IP Phone 7925G. The table shows the network configuration option for the phone that corresponds to the AP configuration.

Table 2-7 Authentication and Encryption Schemes

Cisco AP Configuration			Cisco Unified Wireless IP Phone 7925G Configuration
Authentication	Key Management	Common Encryption	Authentication
Open		None	Open
Open (Static WEP)		WEP	Open+WEP
Shared key (Static WEP)		WEP	Shared+WEP
LEAP 802.1x	Optional CCKM	WEP	LEAP or Auto (AKM)
LEAP WPA	WPA with Optional CCKM	TKIP	LEAP or Auto (AKM)
LEAP WPA2	WPA2	AES	LEAP or Auto (AKM)
EAP-FAST 802.1x	Optional CCKM	WEP	EAP-FAST
EAP-FAST with WPA	WPA Optional CCKM	TKIP	EAP-FAST

Table 2-7 Authentication and Encryption Schemes (continued)

Cisco AP Configuration			Cisco Unified Wireless IP Phone 7925G Configuration
Authentication	Key Management	Common Encryption	Authentication
EAP-FAST with WPA2	WPA2	AES	EAP-FAST
EAP-TLS 802.1x	Optional CCKM	WEP	EAP-TLS
EAP-TLS WPA	WPA with optional CCKM	TKIP	EAP-TLS
EAP-TLS WPA2	WPA2	AES	EAP-TLS
PEAP 802.1x	Optional CCKM	WEP	PEAP
PEAP WPA	WPA with optional CCKM	TKIP	PEAP
PEAP WPA2	WPA2	AES	PEAP
WPA Open and Network EAP	WPA Optional CCKM	TKIP	Auto (AKM) with WPA
WPA-PSK	WPA-PSK	TKIP	Auto (AKM)
WPA2-PSK	WPA2-PSK	AES	Auto (AKM)

For additional information about Cisco WLAN Security, refer to

http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_brochure09186a00801f7d0b.html

For more information about configuring authentication and encryption schemes on APs, refer to the *Cisco Aironet Configuration Guide* for your model and release at this URL:

http://www.cisco.com/en/US/products/hw/wireless/ps4570/products_installation_and_configuration_guides_list.html

Related Topics

- [Networking Protocols Used with Cisco Unified Wireless IP Phones, page 2-9](#)
- [Authentication Methods, page 2-16](#)
- [Encryption Methods, page 2-18](#)
- [Interacting with Cisco Unified Communications Manager, page 2-14](#)
- [Components of the VoIP Wireless Network, page 2-9](#)
- [VoIP WLAN Configuration, page 2-21](#)

VoIP WLAN Configuration

This section provides configuration guidelines for deploying wireless IP phones in the WLAN and includes these topics:

- [Wireless Network Requirements for VoIP, page 2-21](#)
- [VoIP WLAN Configuration, page 2-21](#)

Wireless Network Requirements for VoIP

The Cisco Unified Wireless IP Phone 7925G supports Cisco Aironet APs (APs) that can run Cisco IOS in autonomous mode and APs that run in lightweight mode with lightweight AP protocol (LWAPP) and use a Cisco Unified wireless LAN controller. [Table 2-8](#) lists the supported AP models and operation mode in the WLAN.

When configuring VoWLAN, use APs that run Cisco IOS Release 12.3(8)JA or later. It is recommended that Cisco Aironet 1130AG, 1240AG, 1250 series APs run Cisco IOS Release 12.3(4g)JA1 or later.

Controllers should be running version 4.0217.0 (minimum) or version 4.2.61.0 or later, which is recommended. The controllers should have Cisco IOS Release 12.3(8)JX or later configured also.



Note

Voice over the wireless LAN (VoWLAN) does not currently support MESH technology such as Cisco Aironet 1500 Series Lightweight Outdoor Mesh APs or third-party APs are not supported.

Table 2-8 Supported APs and Modes

AP Models	Autonomous Mode	Lightweight Mode
Cisco Aironet 500 Series	Yes	Yes
Cisco Aironet 1100 Series	Yes	Yes
Cisco Aironet 1130AG Series	Yes	Yes
Cisco Aironet 1200 Series	Yes	Yes
Cisco Aironet 1230 Series	Yes	Yes
Cisco Aironet 1240AG Series	Yes	Yes
Cisco Aironet 1250 Series	Yes	Yes
Cisco Aironet 1300 Series	Yes	Yes
Cisco 1000 Series Lightweight	No	Yes



Note

Be aware that Wi-Fi compliant APs that are manufactured by third-party vendors can function with the Cisco Unified Wireless IP Phone 7925G, but might not support key features such as Dynamic Transmit Power Control (DTPC), ARP-caching, LEAP/EAP-FAST, QBSS, U-APSD, 802.11d and 802.11h.

Configuring the Wireless Network for Voice

This section identifies key AP configuration options that are required for optimal voice performance. This is not a complete list of configuration steps or options for deploying APs such as the Cisco Aironet APs. For more information about configuring your AP, refer to the appropriate Cisco Aironet AP installation and configuration guide for your model or the documentation for your AP.



Note

When deploying the Cisco Unified Wireless IP Phone 7925G with World regulatory domain (CP-7925GW-K9), you must enable the APs for world mode (802.11d). The world model phone gets the channels and power information from the AP.

To see a list of configuration tasks for the Cisco Aironet AP, controller, and Ethernet switch when setting up VoIP on the WLAN, see the [“Configuring a Wireless Network” section on page D-1](#).

Configuration Tip for Cisco Aironet APs

If you are using EAP-FAST, you must increase the EAP request (802.1x) timeout to at least 20 seconds to ensure that the phone gets the PAC credentials successfully.

To change the request timeout on the controller, follow these steps:

Procedure

-
- Step 1** Use SSH or Telnet to access the Cisco Unified wireless LAN controller.
 - Step 2** Enter `config advanced eap request-timeout 20`
 - Step 3** Enter `save config`
 - Step 4** Enter `y` to confirm.
-

Site Survey Verification

Before the initial deployment of wireless phones in the WLAN, it is recommended that a site survey is performed to verify that the APs are providing adequate coverage and that wireless phones can roam from one AP to another with no audio problems. After the initial deployment, it is a good practice to perform site surveys at regular intervals to ensure continued coverage and roaming.

From the Cisco Unified Wireless IP Phone 7925G, you can use the Neighbor List utility or Site Survey utility from the **SETTINGS > Status** menu.

The Neighbor List utility provides information about the current AP and the closest neighbors tracked by the phone. For more information see [Using the Neighbor List Utility, page 2-23](#).

The Site Survey utility produces a report, written as a temporary HTML file, upon termination of the survey. This Site Survey Report is accessible from the phone web page for viewing or forwarding to Cisco TAC for troubleshooting purposes. For more information, see [Using the Site Survey Utility, page 2-24](#).

You should use the wireless IP phone and the Aironet Client Utility (ACU) to verify that the signal range and transmission power provide adequate coverage for roaming phones.

Use the following topics for information about performing the site survey:

- [Performing a Site Survey Verification, page 2-23](#)
- [Using the Neighbor List Utility, page 2-23](#)
- [Using the Site Survey Utility, page 2-24](#)

Performing a Site Survey Verification

Perform these tasks to verify wireless voice network operation. Check that the wireless IP phones:

1. Associate with all APs in the WLAN.
2. Authenticate with all APs in the WLAN.
3. Register with Cisco Unified Communications Manager.
4. Can make stationary phone calls with good quality audio.
5. Can make roaming phone calls with good quality audio and no disconnections.
6. Can place multiple calls, especially in areas designated for high density use.

After phones are installed, request that users report any problems when using their wireless IP phones.

When you perform a site survey verification and encounter problems, see the [Chapter 10, “Troubleshooting the Cisco Unified Wireless IP Phone 7925G”](#) for assistance with finding the cause of the problem.

Related Topics

- [Using the Neighbor List Utility, page 2-23](#)
- [Using the Site Survey Utility, page 2-24](#)

Using the Neighbor List Utility

The Neighbor List utility displays a list of the current AP and the closest neighbors tracked by the phone. The phone typically does not scan while it is idle, so often there is only one entry, which is the currently associated AP, in the list.

To use the Neighbor List utility, follow these steps:

Procedure

-
- Step 1** Configure the Cisco Unified Wireless IP Phone 7925G with the same SSID and encryption/authentication settings as the APs.
 - Step 2** Power on the phone so that it associates with the WLAN.
 - Step 3** Choose **SETTINGS > Status > Neighbor List**.

The phone displays the current AP and the closest neighbors. For example:

SSID: abcd

Channel	BSSID	RSSI	Channel Utilization
01	19:50	-38	50
06	cf:d0	-51	38
11	7b:b0	-42	61

- Step 4** To see more information about an AP, scroll to the desired line and press **Details**. The following is an example of the details for a specific AP:

```
SSID: abcd
Channel:06
BSSID: 00:13:1a:16:cf:d0
RSSI: -51
CU:38
```

- Step 5** To verify the ability to roam between APs, walk through all areas where phones are used and take readings. Approach areas from different directions to assure successful roaming conditions.
- Step 6** Adjust AP and antenna placement and AP power settings to provide approximately 20 percent coverage overlap.

Using the Site Survey Utility

The Site Survey utility is used to actively and passively scan the wireless medium across all channels and locate APs that belong to the Basic Service Set (BSS). The results of the scans are then used help to identify areas of low coverage, if any, and to determine whether the APs are configured consistently as recommended in the Cisco deployment guidelines.

When you start the Site Survey utility, the phone disassociates from the current AP and remains disassociated for the duration of the operation.

For more information, see [Viewing the Site Survey Report on the Web, page 4-38](#).



Caution

During Site Survey, both active and passive scans are performed at a rapid rate. These scans will result in the phone battery life depleting faster than normal and might cause disruption to the wireless medium.

To use the Site Survey utility, follow these steps:

Procedure

- Step 1** Configure the Cisco Unified Wireless IP Phone 7925G with the same SSID and encryption/authentication settings as the APs.
- Step 2** Power on the phone so that it associates with the WLAN.
- Step 3** Choose **SETTINGS > Status > Site Survey**.

The phone displays a list of APs within range that have the same SSID and security settings as the phone. To see more information about an AP, scroll to the desired line and press **Details**.

- Step 4** To verify the ability to roam between APs, walk through all areas where phones are used and take readings. Approach areas from different directions to assure successful roaming conditions.
- Step 5** Adjust AP and antenna placement and AP power settings to provide approximately 20 percent coverage overlap.
- Step 6** When you terminate the site survey, a report is generated for your viewing from the phone web page. For more information, see [Viewing the Site Survey Report on the Web, page 4-38](#).
-

In addition to the Site Survey utility in the Cisco Unified Wireless IP Phone 7925G, you can also use the Cisco Aironet Client Utility Site Survey Utility from a laptop PC. Refer to the section on “Performing a Site Survey” in the *Cisco Aironet Wireless LAN Client Adapters Installation and Configuration Guide* for your system.

Related Topics

- [Performing a Site Survey Verification, page 2-23](#)
- [Viewing the Site Survey Report on the Web, page 4-38](#)



CHAPTER 3

Setting Up the Cisco Unified Wireless IP Phone 7925G

This chapter includes the following topics, which help you install and configure the Cisco Unified Wireless IP Phone 7925G on an IP telephony network:

- [Before You Begin, page 3-1](#)
- [Installing the Cisco Unified Wireless IP Phone 7925G, page 3-7](#)
- [Understanding the Phone Startup Process, page 3-17](#)

Before You Begin

Before installing a Cisco Unified Wireless IP Phone 7925G, review the requirements in these sections:

- [Network Requirements, page 3-1](#)
- [Methods for Adding Phones to Cisco Unified Communications Manager, page 3-2](#)
- [Device Support, page 3-5](#)
- [Safety Information, page 3-5](#)

Network Requirements

For the Cisco Unified Wireless IP Phone 7925G to successfully operate as a Cisco Unified IP Phone endpoint, your network must support these requirements:

Voice over Wireless LAN

- Cisco Aironet Access Points (APs) configured to support Voice over WLAN (VoWLAN)
- Controllers and switches configured to support VoWLAN
- Security implemented for authenticating wireless voice devices and users



Note

You must verify that your wireless network is configured properly for voice service. For more information, see the [“Performing a Site Survey Verification”](#) section on [page 2-23](#).

VoIP Network

- Cisco routers and gateways configured for VoIP
- One of these call-control products installed and configured:
 - Cisco Unified Communications Manager Release 4.3, 5.1, 6.0(1), 6.1(1), or 7.0(1)
 - Cisco Unified Communications Manager Express 4.3 or later
- IP network configured to support DHCP or manual assignment of IP address, gateway, and subnet mask

Related Topics

- [Features Supported on the Cisco Unified Wireless IP Phone 7925G, page 1-6](#)
- [Understanding the Wireless LAN, page 2-1](#)
- [Methods for Adding Phones to Cisco Unified Communications Manager, page 3-2](#)
- [Installing the Cisco Unified Wireless IP Phone 7925G, page 3-7](#)
- [Powering On the Cisco Unified Wireless IP Phone 7925G, page 3-15](#)

Methods for Adding Phones to Cisco Unified Communications Manager

Before installing the wireless IP phone, you must choose a method for adding phones to the Cisco Unified Communications Manager database. Some methods require entering the MAC address of the phone. [Table 3-1](#) provides an overview of these methods.

Table 3-1 *Methods for Adding Phones to the Cisco Unified Communications Manager Database*

Method	Requires MAC Address?	Notes
Auto-registration	No	Results in automatic assignment of directory numbers
Auto-registration with the Tool for Auto-Registered Phones Support (TAPS)	No	Requires auto-registration and Bulk Administration Tool (BAT); updates information in the Cisco Unified IP Phone and in Cisco Unified Communications Manager Administration
BAT	Yes	Allows for simultaneous registration of multiple phones
Cisco Unified Communications Manager Administration only	Yes	Requires phones to be added individually

The following sections describe methods for adding phones:

- [Adding Phones with Auto-Registration, page 3-3](#)
- [Adding Phones with Auto-Registration and TAPS, page 3-3](#)
- [Adding Phones with BAT, page 3-4](#)
- [Adding Phones with Cisco Unified Communications Manager Administration, page 3-4](#)

Adding Phones with Auto-Registration

Use auto-registration to enter phones into the Cisco Unified Communications Manager database without first gathering MAC addresses from the phones. When auto-registration is enabled, Cisco Unified Communications Manager automatically assigns the next available sequential directory number (DN) to new phones during the initial phone startup process.

After registering the phones, you can modify settings, such as the DNs and device pools, by using Cisco Unified Communications Manager Administration.

**Note**

Auto-registration is disabled by default in Cisco Unified Communications Manager Administration. You must enable and properly configure auto-registration before connecting any Cisco Unified IP Phone to the network. For information about enabling and configuring auto-registration, refer to *Cisco Unified Communications Manager Administration Guide*.

Related Topics

- [Adding Phones with Auto-Registration and TAPS, page 3-3](#)
- [Adding Phones with BAT, page 3-4](#)
- [Adding Phones with Cisco Unified Communications Manager Administration, page 3-4](#)

Adding Phones with Auto-Registration and TAPS

Use auto-registration and TAPS to add phones to the Cisco Unified Communications Manager database. Add the phones first by using BAT to the Cisco Unified Communications Manager database with dummy MAC addresses. Then use TAPS to update MAC addresses and download pre-defined configurations for the phones.

To implement TAPS, dial a TAPS DN and follow voice prompts. When the process is complete, the phone has downloaded its DN and other settings. The correct MAC address for the phone is updated in Cisco Unified Communications Manager Administration.

**Note**

You must enable auto-registration in Cisco Unified Communications Manager Administration for TAPS to function.

For Cisco Unified Communications Manager Release 5.0 and prior releases, refer to *Bulk Administration Tool User Guide for Cisco Unified Communications Manager* for detailed instructions about BAT and TAPS. For Cisco Unified Communications Manager Release 6.0(1), 6.1(1), and 7.0(1) refer to *Cisco Unified Communications Manager Bulk Administration Guide*.

Related Topics

- [Adding Phones with Auto-Registration, page 3-3](#)
- [Adding Phones with Cisco Unified Communications Manager Administration, page 3-4](#)
- [Adding Phones with BAT, page 3-4](#)

Adding Phones with BAT

Add a group of phones to the Cisco Unified Communications Manager database by using BAT. This tool performs batch operations, including registration, on multiple phones. You need the MAC addresses for each phone before you use BAT.

[Table 3-2](#) describes how to determine the MAC address of the wireless IP phone.

Table 3-2 Determining the MAC Address of the Phone

Method	For More Information
Choose SETTINGS > Model Information > MAC Address and look at the MAC Address field.	See “Viewing Model Information” section on page 8-7
Remove the battery and look on the back of the phone.	See the “Installing or Removing the Phone Battery” section on page 3-8



Note

BAT is included in Cisco Unified Communications Manager 5.0 or later, but it is a plug-in for prior releases.

For detailed instructions about using BAT, refer to the following documents:

- For Cisco Unified Communications Manager Release 5.0 and prior releases, refer to *Bulk Administration Tool User Guide for Cisco Unified Communications Manager*.
- For Cisco Unified Communications Manager Release 6.0(1), 6.1(1), and 7.0(1), refer to *Cisco Unified Communications Manager Bulk Administration Guide*.



Note

When using BAT to add Cisco Unified Wireless IP Phones, use the default setting for the phone load. The phone load name includes symbols (-, _,.) and BAT does not permit symbols in an entry.

Related Topics

- [Adding Phones with Auto-Registration, page 3-3](#)
- [Adding Phones with Auto-Registration and TAPS, page 3-3](#)
- [Adding Phones with Cisco Unified Communications Manager Administration, page 3-4](#)

Adding Phones with Cisco Unified Communications Manager Administration

Add phones individually by using Cisco Unified Communications Manager Administration. To do so, obtain the MAC address for each phone before you begin. See the [“Methods for Adding Phones to Cisco Unified Communications Manager” section on page 3-2](#) for instructions.

Perform one of the following after collecting the MAC addresses:

- Cisco Unified Communications Manager 5.0, 6.0(1), 6.1(1), or 7.0(1)—Choose **Device > Phone** and click **Add New**.
- Cisco Unified Communications Manager 4.x—Choose **Device > Add a New Device**.

For additional 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 3-3](#)
- [Adding Phones with Auto-Registration and TAPS, page 3-3](#)
- [Adding Phones with BAT, page 3-4](#)

Device Support

Cisco Unified Communications Manager Release 4.1, 4.2, 4.3, 5.1, 6.0, 6.1, and 7.0(1) require a device package or service release update installed to enable device support for the Cisco Unified Wireless IP Phone 7925G. Device packages including support for the Cisco Unified Wireless IP Phone 7925G are available at <http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml>.

Safety Information

Review the following warnings before installing the Cisco Unified IP Phone. To see translations of these warnings, refer to the *Regulatory Compliance and Safety Information for the Cisco Unified Wireless IP Phone 7920G and Peripheral Devices* document that accompanied this device.



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

Statement 1071



Read the installation instructions before connecting the system to the power source. Statement 1004



This equipment will not be able to access emergency services during a power outage because of reliance on utility power for normal operation. Alternative arrangements should be made for access to emergency services. Access to emergency services can be affected by any call-barring function of this equipment.



Do not use the Cisco Unified Wireless IP Phone 7925G in hazardous environments such as areas where high levels of explosive gas may be present. Check with the site safety engineer before using any type of wireless device in such an environment.



The plug-socket combination for the battery charger must be accessible at all times, because it serves as the main disconnecting device. Statement 1019

**Warning**

The battery charger requires short-circuit (overcurrent) protection to be provided as part of the building installation. Install only in accordance with national and local wiring regulations. Statement 1045

**Warning**

The power supply must be placed indoors. Statement 331

**Warning**

Ultimate disposal of this product should be handled according to all national laws and regulations. Statement 1040

**Warning**

Telephone receivers produce a magnetic field that can attract small magnetic objects such as pins and staples. To avoid the possibility of injury, do not place the handset where such objects may be picked up.

Battery Safety Notices

The following battery safety notices apply to the batteries that are approved by the Cisco Unified Wireless IP Phone 7925G manufacturer.

**Warning**

There is the danger of explosion if the battery is replaced incorrectly. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions. Statement 1015

**Warning**

Do not dispose of the battery pack in fire or water. The battery may explode if placed in a fire.

**Caution**

The battery pack is intended for use only with this device.

**Caution**

Do not disassemble, crush, puncture, or incinerate the battery pack.

**Caution**

To avoid risk of fire, burns, or damage to your battery pack, do not allow a metal object to touch the battery contacts.

**Caution**

Handle a damaged or leaking battery with extreme care. If you come in contact with the electrolyte, wash the exposed area with soap and water. If the electrolyte has come in contact the eye, flush the eye with water for 15 minutes and seek medical attention.

**Caution**

Do not charge the battery pack if the ambient temperature exceeds 104 degrees Fahrenheit (40 degrees Celsius).

**Caution**

Do not expose the battery pack to high storage temperatures (above 140 degrees Fahrenheit, 60 degrees Celsius).

**Caution**

When discarding a battery pack, contact your local waste disposal provider regarding local restrictions on the disposal or recycling of batteries.

To obtain a replacement battery, contact your local dealer. Use only the batteries that have the following Cisco part numbers.

Standard battery—CP-BATT-7925G-STD

Extended battery—CP-BATT-7925G-EXT

**Caution**

Use only the Cisco power supply. If you must replace your power supply, refer to the list of Cisco part numbers.

Australia—CP-PWR-7925G-AU

Central Europe—CP-PWR-7925G-CE

China—CP-PWR-7925G-CN

Japan—CP-PWR-7925G-JP

North America—CP-PWR-7925G-NA

United Kingdom—CP-PWR-7925G-UK

Related Topics

- [Network Requirements, page 3-1](#)
- [Providing Power to the Phone, page 3-7](#)

Installing the Cisco Unified Wireless IP Phone 7925G

After setting up the wireless network to support voice communications and configuring the wireless IP phones in Cisco Unified Communications Manager, you are ready to install the phones. This section includes the following installation information:

- [Providing Power to the Phone, page 3-7](#)
- [Configuring Wireless LAN Settings for the Cisco Unified Wireless IP Phone 7925G, page 3-13](#)
- [Using a Headset, page 3-13](#)

Providing Power to the Phone

The Cisco Unified Wireless IP Phone 7925G uses a battery for power. [Table 3-3](#) lists the types of batteries available for the wireless IP phone and the maximum talk and standby times.

Table 3-3 Batteries Available for the Cisco Unified Wireless IP Phone 7925G

Type	Technology	Talk Time	Standby Time
Standard	Lithium ion (Li-ion)	Up to 9.5 hrs	Up to 180 hrs
Extended	Li-ion	Up to 13 hrs	Up to 240 hrs

Use U-APSD for talk-time power save mode. Also 5 GHz talk time is reduced up to 30 min for standard and up to 2 hours for extended. Use of 802.11b/g and a Bluetooth headset can reduce the talk time by 40-50 percent. To extend talk-time battery life, the Cisco Unified Wireless IP Phone 7925G can use PS-POLL power save methods. The Cisco Unified Wireless IP Phone 7925G will use either U-APSD or PS-POLL when in idle (no active phone call).

When an AP supports the Cisco Client Extensions (CCX) proxy ARP information element, the idle battery life is optimized. If the AP does not support CCX or proxy ARP is not enabled, then the idle battery life is up to fifty percent less.

[Table 3-4](#) shows the charging time for the two types of batteries. You can stop charging the battery when the battery is fully charged. Lithium ion batteries can be partially charged without shortening the battery life. Batteries should handle up to 4000 recharges.

**Note**

Battery life varies because of environmental factors and Bluetooth use.

Table 3-4 Battery Charging Time Information

Battery Type	Power Supply Connected to Phone	Phone Connected to PC and USB Cable
Standard	2 hours	5 hours
Extended	3 hours	7 hours

The following sections provide information about the battery and charging the phone:

- [Installing or Removing the Phone Battery, page 3-8](#)
- [Using the Power Supply to Charge the Phone Battery, page 3-11](#)
- [Using the USB Cable and PC to Charge the Battery, page 3-12](#)

Installing or Removing the Phone Battery

To install the battery in the Cisco Unified Wireless IP Phone use [Figure 3-1](#), and follow these steps:

Procedure

-
- Step 1** Remove the cover on the back of the phone as shown in [Figure 3-1](#).
 - Step 2** To install the battery, insert the battery catches in the corresponding slots at the bottom of the Cisco Unified Wireless IP Phone 7925G. Ensure that the metal contacts on the battery and the phone are facing each other.
 - Step 3** Press the battery to the body of the phone until it locks into place. See [Figure 3-2](#).

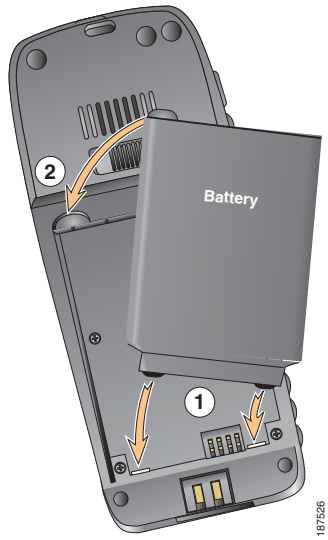
Step 4 To remove the battery, press up on the locking catch, then lift and remove the battery as shown in [Figure 3-3](#).

Figure 3-1 Removal of Cover to Install the Battery

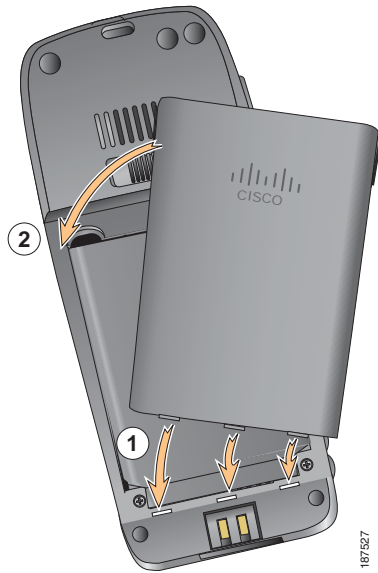


1	Locking catch
2	Battery Cover

Figure 3-2 Install the Battery



1	Battery Insertion Slots
2	Battery

Figure 3-3 Replace the Back Cover

1	Cover Insertion Slots
2	Cover

**Note**

The MAC address for each Cisco Unified Wireless IP Phone 7925G appears on a printed label on the back of the phone underneath the battery.

Using the Power Supply to Charge the Phone Battery

To charge the phone battery quickly, follow the steps in [Figure 3-4](#).

Figure 3-4 Charging the Phone Battery



1	Lift the mini-USB port cover on the bottom of phone.
2	Swing the port cover to one side.
3	Insert the AC power supply mini-USB connector in the port.
4	Insert the AC plug adapter in the slot on the power supply.
5	Insert the AC power supply in a wall outlet.
6	Indicator light—Indicates the charging status: <ul style="list-style-type: none"> • Red—Battery charging in process. • Green—Battery charging is complete.



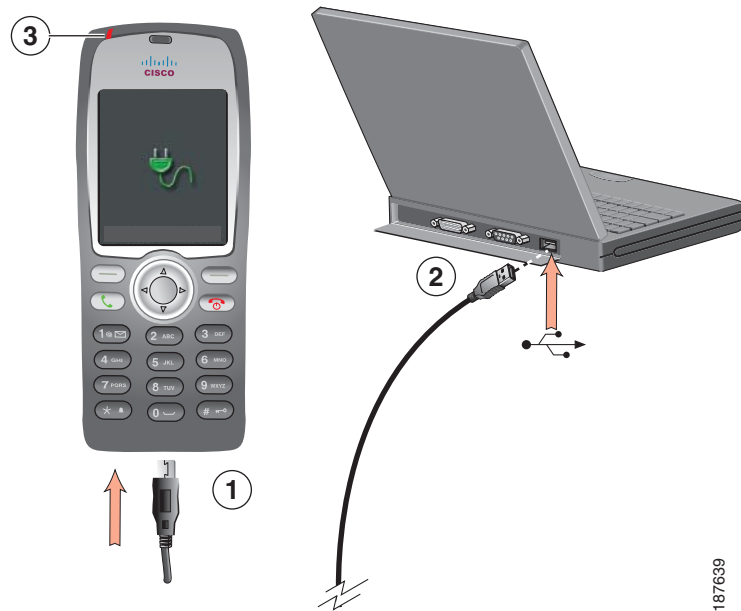
Note

You can use the phone while the battery is being charged. For charging times, see [Table 3-4](#).

Using the USB Cable and PC to Charge the Battery

Charge the phone battery by using a USB cable connected to your PC. Follow the steps in [Figure 3-5](#).

Figure 3-5 Charging the Phone Battery Using the USB Cable and PC



1	Insert the phone connector on the USB cable into the phone.
2	Insert the USB A-type connector into the USB port on your PC.
3	<p>Monitor the indicator light after the phone briefly displays “USB Connected” on the status line.</p> <p>You may see the “Found New Hardware Wizard” To stop the wizard from opening when connecting to USB port, perform the following steps:</p> <ol style="list-style-type: none"> 1. Click Next to use the wizard dialog box. 2. In the Update New Software dialog, click No, not this time, and click Next. 3. Click Install the Software automatically (Recommended) and click Next. 4. After a few moments, the Cannot Install This Hardware dialog displays. Click Don't prompt me again to install this software. 5. Click Finish to close the dialog box.



Note

While the battery is charging, the indicator light is red. When the battery is fully charged, the indicator light turns green. Charging times are longer when you use this method and are described in [Table 3-4](#).

Related Topics

- [Powering On the Cisco Unified Wireless IP Phone 7925G, page 3-15](#)
- [Installing or Removing the Phone Battery, page 3-8](#)

187639

- [Using the Power Supply to Charge the Phone Battery, page 3-11](#)

Configuring Wireless LAN Settings for the Cisco Unified Wireless IP Phone 7925G

Before the phone can connect to the WLAN, you must configure the network profile for the phone with the WLAN settings. You can use two methods for setting up the network profiles:

- [Cisco Unified Wireless IP Phone 7925G Web Pages, page 3-13](#)
- [Network Profile Menu on the Cisco Unified Wireless IP Phone 7925G, page 3-13](#)

Cisco Unified Wireless IP Phone 7925G Web Pages

You can access the Cisco Unified Wireless IP Phone 7925G web pages to set up the WLAN settings in the network profile. For a new phone with the factory default settings, you must use the USB cable to connect the phone to your PC. For more information and instructions, see [Chapter 4, “Using the Cisco Unified Wireless IP Phone 7925G Web Pages.”](#)

Network Profile Menu on the Cisco Unified Wireless IP Phone 7925G

You can use the Settings menu on the phone and access the Network Profiles menu to set up the network configuration and the WLAN configuration. For more information and instructions, see [Chapter 5, “Configuring Settings on the Cisco Unified Wireless IP Phone 7925G.”](#)

Using a Headset

Although Cisco Systems performs some internal testing of third-party wired and Bluetooth wireless headsets for use with the Cisco Unified Wireless IP Phone 7925G, Cisco does not certify or support products from headset or handset vendors. Because of the inherent environmental and hardware inconsistencies in the locations where Cisco Unified IP Phones are deployed, there is not a single “best” solution that is optimal for all environments. Cisco recommends that customers test the headsets that work best in their environment before deploying a large number of units in their network.

Cisco Systems recommends the use of good quality external devices, like headsets that are 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 cell phones and two-way radios, some audio noise may still occur. See [Using External Devices with Cisco Unified IP Phones, page 3-15](#) for more information.

The primary reason that a particular headset would be inappropriate for the Cisco Unified IP Phone is the potential for an audible hum. This hum can be heard by either the remote party or by both the remote party and you, the Cisco Unified IP Phone user. Some potential humming or buzzing sounds can be caused by a range of outside sources, for example, electric lights, being near electric motors, large PC monitors. 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.

Connecting Headsets

To connect a headset to the Cisco Unified Wireless IP Phone 7925G, plug it into the headset port on the right side of the phone.

You can use the headset with all of the features on the Cisco Unified Wireless IP Phone 7925G, 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.

Using Bluetooth Wireless Headsets

The Cisco Unified Wireless IP Phone 7925G supports Bluetooth Class 2 technology with Hands Free version 1.5 when the headsets support Bluetooth. Bluetooth enables low bandwidth wireless connections within a range of 10 meters. The best performance is in the 1 to 2 meter range.

There can be a potential interference issues. It is recommended that you:

- Reduce the proximity of other 802.11b/g devices, Bluetooth devices, microwave ovens, and large metal objects.
- Use the Cisco Unified Wireless IP Phone 7925G on the same side of the body as the Bluetooth-enabled headset.

Using Bluetooth wireless headsets will likely increase battery power consumption on your phone and might result in reducing battery life.

For a Bluetooth wireless headset to work, it does not need to be within direct line-of-sight of the phone, but some barriers, such as walls or doors, and interference from other electronic devices, could affect the connection.

Pairing Headsets

The Cisco Unified Wireless IP Phone 7925G pairs with headsets using a shared key authentication and encryption method. The authentication process can require a personal identification number (PIN) specific to the headset, commonly “0000.” The Cisco Unified Wireless IP Phone 7925G can be paired with more than one headset at a time. Pairing is typically performed once for each headset.

Once a device has been paired, its Bluetooth connection is maintained as long as both devices (phone and headset) are enabled and within range of each other. The connection re-establishes itself automatically if either of the devices powers down then powers up. The green-dotted Bluetooth icon indicates whether or not a device is connected.

When headsets are more than 10 meters away from Cisco Unified Wireless IP Phone 7925G, Bluetooth drops the connection after a 15 to 20 second timeout. If the paired headset comes back into range of the Cisco Unified Wireless IP Phone 7925G and the phone is not connected to another Bluetooth headset, then the in-range Bluetooth headset automatically reconnects. For certain phone types that operate in power-save modes, the user may have to “wake-up” the headset by tapping on its operational button to initiate the reconnect.



Note

It is recommended that users read the headset user guide for more information about pairing and connecting the headsets.

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 is subjective and Cisco cannot guarantee the performance of any headsets, but some of the headsets on the sites listed below have been reported to perform well on Cisco Unified IP Phones.

Nevertheless, it is ultimately the customer's responsibility to test this equipment in their own environment to determine suitable performance.

For information about wired and Bluetooth wireless headsets for your phone, see the *Cisco Unified Wireless IP Phone 7925G Accessory Guide* and these web sites:

- <http://www.plantronics.com>
- <http://www.jabra.com>
- <http://www.jawbone.com>

Using External Devices with Cisco Unified IP Phones

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

- Cisco recommends the use of good quality external devices (speakers, microphones, and headsets) that are shielded (screened) against unwanted radio frequency (RF) and audio frequency (AF) signals.
- Depending on the quality of these devices and the 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 speakers, microphones, and headsets that are fully compliant with the EMC Directive [89/336/EC].

Powering On the Cisco Unified Wireless IP Phone 7925G

After charging the battery and configuring the wireless IP phone, you are ready to power on the phone and connect to the WLAN. Use the following sections for more information about starting up the phone.

- [Active and Standby Phone Modes, page 3-16](#)
- [Understanding the Phone Startup Process, page 3-17](#)

To power on the Cisco Unified Wireless IP Phone 7925G, press and hold the Power On button until the phone begins its startup process by cycling through these steps:

1. The phone displays the Cisco Systems screen.
2. The phone screen displays these messages as the phone starts up:
 - Locating Network Services
 - Configuring IP
 - Network Up
 - Configuring Unified CMList
 - Registering
3. The following information displays on the main phone screen:
 - Current time and date
 - Primary directory number
 - Main screen icons for four menus and Help
 - “Your current options” on status line
 - Softkey labels (Messages and Options)

When the phone passes through these stages with no errors, the phone started up properly. Now the phone is in standby mode and is ready to place or receive calls.

The signal icon in the upper left corner shows the strength of the signal between the wireless access point and the phone. The phone must have an adequate signal to successfully place or receive calls. If the signal icon displays only one bar, the weak signal can cause problems with phone performance.

If the phone does not complete these steps successfully, see the [“Resolving Startup and Connectivity Problems”](#) section on page 10-1.

Related Topics

- [Active and Standby Phone Modes, page 3-16](#)
- [Understanding the Phone Startup Process, page 3-17](#)

Active and Standby Phone Modes

When the Cisco Unified Wireless IP Phone 7925G is powered on, it can be in one of these two modes:

- Active mode
- Standby mode

Active Mode

The phone is in active mode when there is an active RTP stream. When the phone is performing one of these actions, it is consuming power:

- Connected to an active call
- Scanning for channels
- Sending CDP packets
- Sending keep-alive messages

- Reregistering with Cisco Unified Communications Manager

The standard battery provides up to 11.5 hours of talk time in active mode and the extended battery provides up to 15.5 hours of talk time.

Standby Mode

The phone goes into standby mode two seconds after a scan is complete. The phone awakes from standby mode in response to these events:

- Pressing keys on the keypad
- Roaming between APs
- Power cycling the phone
- Losing network connectivity
- Losing RF connectivity
- Transmitting scheduled CDP or keep-alive packets.

The standard battery provides up to 150 hours of standby time and the extended battery provides up to 200 hours of standby time.

Related Topics

- [Understanding the Phone Startup Process, page 3-17](#)
- [Resolving Startup and Connectivity Problems, page 10-1](#)

Understanding the Phone Startup Process

When connecting to the wireless VoIP network, the Cisco Unified Wireless IP Phone 7925G goes through a standard startup process, as described in [Table 3-5](#). Depending on your specific network configuration, not all of these steps may occur on your wireless IP phone.

Table 3-5 Cisco Unified Wireless IP Phone Startup Process

Step	Description	Related Topics
1. Powering on the phone	The Cisco Unified Wireless IP Phone 7925G 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.	Providing Power to the Phone, page 3-7 Resolving Startup and Connectivity Problems, page 10-1
2. Scanning for an access point	The Cisco Unified Wireless IP Phone 7925G scans the RF coverage area with its radio. The phone searches its network profiles and scans for access points that have a matching SSID and authentication type. The phone associates with the access point with the highest RSSI that matches with its network profile.	Interacting with Cisco Unified Wireless APs, page 2-11 Resolving Startup and Connectivity Problems, page 10-1

Table 3-5 Cisco Unified Wireless IP Phone Startup Process (continued)

Step	Description	Related Topics
3. Authenticating with access point	<p>The Cisco Unified Wireless IP Phone 7925G begins the authenticating process.</p> <ul style="list-style-type: none"> • If set for Open, then any device can authenticate to the access point. For added security, static WEP encryption might optionally be used. • If set to Shared Key, the phone encrypts the challenge text using the WEP key and the access point must verify that the WEP key was used to encrypt the challenge text before network access is available. • If set for LEAP or EAP-FAST, then the user name and password are authenticated by the RADIUS server before network access is available. • If set for Auto (AKM), the phone looks for an access point with one of the following key management options enabled: <ul style="list-style-type: none"> – WPA, WPA2, or CCKM—The username and password are authenticated by the RADIUS server before network access is available. – WPA-Pre-shared key, WPA2-Pre-shared key—The phone authenticates with the access point using the pre-shared key. 	<p>Authentication Methods, page 2-16</p>
4. Configuring IP network	<p>If the wireless 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 a static IP address to each phone locally.</p> <p>In addition to assigning an IP address, the DHCP server directs the wireless IP phone to a TFTP server. If the phone has a statically defined IP address, you must configure the TFTP server IP address locally on the phone; the phone then contacts the TFTP server directly.</p>	<ul style="list-style-type: none"> • Configuring DHCP Settings, page 5-6 • Disabling DHCP, page 5-6 • Resolving Startup and Connectivity Problems, page 10-1
5. Downloading Load ID	<p>The wireless IP phone checks to verify that the proper firmware is installed or if new firmware is available to download.</p> <p>Cisco Unified Communications Manager informs devices using .cnf or .cnf.xml format configuration files of their load ID. Devices using .xml format configuration files receive the load ID in the configuration file.</p>	<ul style="list-style-type: none"> • Phone Configuration Files and Profile Files, page 2-14
6. Downloading config file	<p>The TFTP server has configuration files and profile files. A configuration file includes parameters for connecting to Cisco Unified Communications Manager and information about which image load a phone should be running. A profile file contains various parameters and values for phone and network settings.</p>	<ul style="list-style-type: none"> • Configuring an Alternate TFTP Server, page 5-7 • Phone Configuration Files and Profile Files, page 2-14 • Resolving Startup and Connectivity Problems, page 10-1

Table 3-5 Cisco Unified Wireless IP Phone Startup Process (continued)

Step	Description	Related Topics
7. Connecting to Cisco Unified Communications Manager	The configuration file defines how the Cisco Unified IP Phone communicates with Cisco Unified Communications Manager. After obtaining the file from the TFTP server, the phone attempts to make a TCP connection to the highest priority Cisco Unified Communications Manager on the list.	<ul style="list-style-type: none"> • Interacting with Cisco Unified Communications Manager, page 2-14 • Resolving Startup and Connectivity Problems, page 10-1
8. Registering to Cisco Unified Communications Manager	If the phone was manually added to the database, Cisco Unified Communications Manager identifies and registers 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.	<ul style="list-style-type: none"> • Overview of Configuring and Installing the Cisco Unified Wireless IP Phone 7925G, page 1-14 • Adding Users to Cisco Unified Communications Manager, page 7-19

Related Topics

- [Configuring Cisco Unified Wireless IP Phones in Cisco Unified Communications Manager, page 7-1](#)
- [Phone Configuration Files and Profile Files, page 2-14](#)



CHAPTER 4

Using the Cisco Unified Wireless IP Phone 7925G Web Pages

This chapter describes how to set up your PC to configure a Cisco Unified Wireless IP Phone 7925G by using a USB connector and how to remotely access a configured phone over the WLAN. It contains the following sections:

- [Setting Up Your PC to Configure the Phones, page 4-1](#)
- [Updating the Phones Remotely, page 4-4](#)
- [Configuring Network Profiles, page 4-8](#)
- [Configuring USB Settings, page 4-26](#)
- [Configuring Trace Settings, page 4-27](#)
- [Configuring the Phone Book, page 4-29](#)
- [Configuring Wavelink Settings, page 4-29](#)
- [Using System Settings, page 4-34](#)

Setting Up Your PC to Configure the Phones

To setup new phones, use your PC and USB connection to enter the initial configuration for the wireless network settings and network profiles. To save time during initial deployment, you can create a standard network profile template and export it to several phones. For more information, see the [“Backup Settings for Phone Configuration”](#) section on page 4-34.

Before you can configure phones by using the USB connection, you must install drivers and set up the USB ports on the phone and PC.

Your PC must have one of the following operating systems:

- Windows 2000 Professional
- Windows XP

Installing the USB Drivers

To install the drivers on your PC, perform the following steps:

Procedure

-
- Step 1** Log into Cisco.com.
- Step 2** Download the installation package and “read me” file for the USB drivers from this location:
<http://www.cisco.com/cgi-bin/tablebuild.pl/ip-7900ser-crypto>



Note Before proceeding, review the “read me” file for specific instructions for your PC operating system.

- Step 3** Double-click on the **USB-Install-7925.1-0-2.exe** file to start the installation program.
- Step 4** Follow the prompts in the InstallShield Wizard.



Note If you receive a Hardware Installation warning message stating that the software has not passed Microsoft Windows Logo testing, click **Continue**.

- Step 5** The driver installation is complete when you see the Finished screen. You can close the wizard.
- Step 6** Plug the USB cable into the USB port on the PC and into the USB connector on the phone.
 The Found New Hardware Wizard dialog opens.
- Step 7** To update the new software, click the button next to **Yes, this time only** and click **Next**.
- Step 8** Click the button next to **Install the Software automatically (Recommended)**.
 After 2-3 minutes, the software installs and a message appears on the task bar stating “Found New Hardware - Software installed and ready to use.”
- Step 9** Click **Finish** when the installation is complete.
 The phone briefly displays “USB Connected” on the status line.
-

Configuring the USB LAN on the PC

To configure the USB LAN connection on your PC, follow these steps:

Procedure

-
- Step 1** To setup the USB LAN connection, do one of the following:
- For Windows XP—Click **Start > Settings > Control Panel > Network Connections**.
 - For Windows 2000—Click **Start > Settings > Control Panel > Network and Connections**.
- Step 2** Locate and double-click the new LAN connection to open the Local Area Connection Status window, then click **Properties**.
- Step 3** Scroll to the Internet Protocol (TCP/IP) section and click **Properties**.

Step 4 In the Internet Protocol (TCP/IP) Properties window, choose **Use the following IP address:**

Step 5 In the IP address field, enter a static IP address for the PC: **192.168.1.** (1 through 254 except 100), for example: 192.168.1.11

**Note**

- By default, the Cisco Unified Wireless IP Phone 7925G is configured with 192.168.1.100 so you cannot use this IP address for the PC.
- Make sure to use an IP address that is not in use on any other interface on the PC.

Step 6 Enter the subnet mask: **255.255.255.0**

Step 7 Click **OK** to make the changes.

Related Topics

- [Accessing the Phone Web Page, page 4-3](#)
- [Setting Configuration Privileges for the Phone Web Page, page 4-4](#)
- [Accessing the Configuration Web Page for a Phone, page 4-5](#)
- [Summary Information on the Home Web Page, page 4-7](#)

Accessing the Phone Web Page

After setting up the USB interface on the PC, you are ready to use the USB cable connection to the phone to access the phone web pages.

To access the phone web pages, follow these steps:

Procedure

Step 1 Open a Windows browser.

Step 2 In the address field, enter **https://192.168.1.100** to locate the wireless IP phone web page.

**Note**

When the Security Alert dialog box displays a notice to accept the Trust Certificate, click **Yes** or **Always** to accept the application.

The Summary web page for the phone displays. See [Table 4-2](#) for details about this web page.

Step 3 Use the hyperlinks in the left column of the web page to configure settings for the phones. For information, see these sections:

- [Configuring Network Profiles, page 4-8](#)
- [Configuring USB Settings, page 4-26](#)
- [Configuring Trace Settings, page 4-27](#)
- [Configuring Wavelink Settings, page 4-29](#)
- [Configuring the Phone Book, page 4-29](#)
- [Using System Settings, page 4-34](#)

- Step 4** After entering the new settings, disconnect the USB cable from the phone. The settings are active immediately.
- Step 5** Check that the phone can access the network successfully.
-

Using the USB Cable to Configure Phones

You are ready to use the USB cable to set up other phones. Before plugging the USB cable into another phone, wait approximately 12-15 seconds for the USB interface on the PC to shut down.

To connect to another phone, follow these steps:

Procedure

- Step 1** Plug the USB cable into a Cisco Unified Wireless IP Phone 7925G.
The phone briefly displays “USB Connected” on the status line.
- Step 2** Access the web page for the new phone by following the steps in [“Accessing the Phone Web Page” section on page 4-3](#).
-

Related Topics

- [Installing the USB Drivers, page 4-2](#)
- [Configuring the USB LAN on the PC, page 4-2](#)
- [Using the USB Cable to Configure Phones, page 4-4](#)
- [Accessing the Phone Web Page, page 4-3](#)

Updating the Phones Remotely

You might have to update settings on a Cisco Unified Wireless IP Phone 7925G that is already configured and in use. You can use the wireless LAN to remotely access and configure these phones.

Use these sections for information about remotely updating phones:

- [Setting Configuration Privileges for the Phone Web Page, page 4-4](#)
- [Accessing the Configuration Web Page for a Phone, page 4-5](#)

Setting Configuration Privileges for the Phone Web Page

To make changes to the phone by using the web page, you must use Cisco Unified Communications Manager Administration to enable Web Access and Phone Book Web Access.

To allow configuration privileges, follow these steps:

Procedure

- Step 1** Log into Cisco Unified Communications Manager Administration.

- Step 2** Search for the phone in Cisco Unified Communications Manager Administration by choosing **Device > Phone** and enter search information such as the DN.
- Step 3** Click on the DN of the phone that you want to set the privileges.
- Step 4** Open the Phone Configuration window, scroll down to Product Specific Configuration Layout, and enable these privileges:
- In the Web Access field, select **Full** from the drop-down menu.
 - In the Phone Book Web Access field, select **Allow Admin**.
- Step 5** Click **Save** to make the change.
- Step 6** You must reset the phone to enable configuration privileges on the web pages for this phone.
-

Accessing the Configuration Web Page for a Phone

You can access the web page for any Cisco Unified Wireless IP Phone 7925G that is connected to the WLAN. Be sure the phone is powered on, connected and registered to a Cisco Unified Communications Manager server.

To access the web page for the Cisco Unified Wireless IP Phone 7925G follow these steps:

Procedure

- Step 1** Log into the Cisco Unified Communications Manager Administration.
- Step 2** Go to **Device > Phone**.
- Step 3** Click **Find**. All of the phones display. If the phone is registered with a Cisco Unified Communications Manager Administration, the IP address displays. The phone IP address is linked to the Home web page.
- Step 4** Click on the **Description** field in the Phone Configuration window of Cisco Unified Communications Manager Administration. The Device Information section displays.
- Step 5** Go to the Web Access field in the Product Specific Configuration Layout and change the parameter to **Full**. This will give you full access to all of the web pages.
- Step 6** From the Phone Configuration window, click on the linked IP address. The Home web page displays. There are two sections displayed on the Home web page: setup menus (left) and summary information (right). [Table 4-1](#) shows the available Home web page menus, from which you can configure network profiles, USB settings, trace settings, Wavelink settings, and certificates. [Table 4-2](#) contains the phone summary information.

Or if you already know the IP address, you can open a web browser and enter the following URL. The *IP_address* variable is the IP address of the Cisco Unified IP Phone:

```
https://<IP_address>/index.html
```



Note When the Security Alert dialog box displays a notice to accept the Trust Certificate, click **Yes** or **Always** to accept the application.

- Step 7** Log into the Home web page with the default username: **admin** and enter the default password: **Cisco**. You may need to log into additional windows to configure other options.
- Step 8** Make changes to configurable pages as needed.

- Step 9** Return to the Phone Configuration page in Cisco Unified Communications Manager Administration and set the Web Access field back to **Read Only** or **Disabled**.
- Step 10** Reset the phone from Cisco Unified Communications Manager to disable full access to the web pages. Be sure to change the Web Access privileges and reset the phone to prevent users from making configuration changes on the phone web pages.

**Note**

If a wireless IP phone was previously registered to Cisco Unified CallManager Administration Release 4.x, and you try to register to Cisco Unified Communications Manager Administration 5.x, 6.0(1), 7.0(1), the Phone Configuration web page password might be set to “Cisco.”

Table 4-1 Home Web Page Menus

Menu	Related Information
Setup	
• Network Profiles	Configuring Network Profiles, page 4-8
• USB Settings	Configuring USB Settings, page 4-26
• Trace Settings	Configuring Trace Settings, page 4-27
• Wavelink Settings	Configuring Wavelink Settings, page 4-29
• Certificates	Configuring Wireless LAN Security, page 4-13
Configurations	
Phone Book	Configuring the Phone Book, page 4-29
Information	
• Network	Summary Information on the Home Web Page, page 4-7
• Wireless LAN	
• Device	
Statistics	
• Wireless LAN	Displays Rx and Tx statistics.
• Network	Displays IP, TCP, and UDP statistics.
Stream Statistics	
• Stream 1	Displays RTP statistics and voice quality metrics.
• Stream 2	

Table 4-1 Home Web Page Menus (continued)

Menu	Related Information
System	
• Trace Logs	Using System Settings, page 4-34
• Backup Settings	
• Phone Upgrade	
• Change Password	
• Site Survey	
• Date and Time	
• Phone Restart	

Summary Information on the Home Web Page

The summary information for your phone displays on this section of the Home web page. It also displays the network and Cisco Unified Communications Manager information. [Table 4-2](#) describes these items.

Table 4-2 Summary Information

Item	Description
Phone DN	DN assigned to the phone.
Home: Summary	
Wireless Information	
Active Network Profile	Name of the profile that the phone is currently using.
SSID	SSID that the phone is currently using.
Access Point	Name of the access point (AP) to which the phone is associated.
MAC Address	MAC address of the phone.
Network Information	
IP Address	IP address of the phone.
Subnet Mask	Subnet mask used by the phone.
Default Router	IP address for the default gateway that the phone is using.
TFTP Server	IP address for the Primary TFTP server that the phone is using.
Call Manager Information	
Active Call Manager	IP address for the Cisco Unified Communications Manager server to which the phone is registered.
Phone Directory Number	Primary DN for the phone.

Related Topics

- [Accessing the Phone Web Page, page 4-3](#)
- [Configuring Network Profiles, page 4-8](#)
- [Configuring USB Settings, page 4-26](#)
- [Configuring Trace Settings, page 4-27](#)

- [Configuring the Phone Book, page 4-29](#)
- [Using System Settings, page 4-34](#)

Configuring Network Profiles

You can configure up to four profiles for a phone to take advantage of WLAN environments. You can add names to the profiles and enable one or more of the profiles for the phone to use. The Network Profiles section of the web page displays the following information about each phone:

- Profile—Displays a list of four configurable profiles.
- Enabled—Indicates whether or not the profile is enabled.
- Name—Lists the name for the profile.
- SSID—Lists the SSID used by the profile.
- Status—Indicates which profiles are active or inactive.

To display the Network Profiles list, access the web page for the phone as described in the [“Accessing the Phone Web Page”](#) section on page 4-3, and then click the **Network Profiles** hyperlink.

For more information about configuring network profiles, see these sections:

- [Configuring Wireless Settings in a Network Profile, page 4-12](#)
- [Configuring Wireless LAN Security, page 4-13](#)
- [Configuring IP Network Settings, page 4-23](#)
- [Configuring the Alternate TFTP Server, page 4-24](#)
- [Configuring Advanced Network Profile Settings, page 4-25](#)

Network Profile Settings

You can configure the settings for a profile by using this web page area. You can also modify or view configured profiles from this web page area. [Table 4-3](#) and [Table 4-4](#) describe the basic and advanced profile settings and provides references for more information.

To display Network Profile (1-4) Settings, access the web page for the phone as described in the [“Accessing the Phone Web Page”](#) section on page 4-3, and then click the **Profile (1-4)** hyperlink.

Table 4-3 Basic Network Profile Settings

Item	Description	For More Information, See...
Wireless		
Profile Name	Descriptive name for the profile.	—
SSID	Assigns the Service Set Identifier (SSID) to this profile. You must assign the same SSID to the phone that is also assigned to access points in the wireless network.	Associating to APs, page 2-12
Edit Profile	Enables editing of the profile.	—

Table 4-3 Basic Network Profile Settings (continued)

Item	Description	For More Information, See...
Scan Mode	<p>Auto—Always scans when on a call. If idle and signal strength is sufficient, the phone does not scan.</p> <p>Continuous—Always scans.</p> <p>Single AP—Only scans at power on or if the AP connection to the network is lost.</p>	Associating to APs, page 2-12
Call Power Save Mode	<p>Set for the type of power saving mode used in the WLAN. Options are:</p> <ul style="list-style-type: none"> • U-APSD/PS-Poll • None 	802.11 Standards for WLAN Communications, page 2-3
802.11 Mode	<p>Determines the signal mode or priority for selecting signal modes available in the WLAN. Options are:</p> <ul style="list-style-type: none"> • 802.11 b/g—Use only 2.4 GHz band • 802.11a—Use only 5 GHz band • Auto, 802.11b/g preferred over 802.11a (dual band) • Auto, 802.11a preferred over 802.11b/g (dual band) <p>Note The preferred band, if available, will be used at power-on, but the phone may switch to the less preferred 2.4 GHz band, if available, and the preferred band is lost. Once the phone has connected to the less preferred band, it will not scan for the preferred band if the current band is acceptable, and may remain connected to the less preferred band.</p> <ul style="list-style-type: none"> • Auto, signal strength (RSSI)—Use strongest signal in dual band environment 	802.11 Standards for WLAN Communications, page 2-3
Restricted Data Rate	<p>Enables or disables the restriction of the upstream and downstream PHY rates according to CCX V4 Traffic Stream Rate Set IE (S54.2.6). The default is disabled.</p>	—

Table 4-3 Basic Network Profile Settings (continued)

Item	Description	For More Information, See...
WLAN Security		
Authentication Mode	Assigns the authentication mode	Configuring Advanced Network Profile Settings, page 4-25
Export Security Credentials	Controls whether the wireless security credential data can be exported in the configuration file. <ul style="list-style-type: none"> • True—Allows exporting the data • False—Blocks exporting the data 	
Wireless Security Credentials		
Username	Assigns the network authentication username for this profile	Configuring the Username and Password, page 4-15
Password	Assigns the network authentication password for this profile	
WPA Pre-shared Key Credentials		
Pre-shared Key Type	Determines the key type: Hex or ASCII	Configuring the Pre-shared Key, page 4-15
Pre-shared Key	Identifies the key	
Wireless Encryption		
Key Type	Determines the encryption key type: Hex or ASCII	Setting Wireless Encryption, page 4-16
Encryption Key 1-4	Identifies the Transmit Key: <ul style="list-style-type: none"> • Encryption Key character string • Key Size of 40 or 128 characters 	
Certificate Options		
Client EAP-TLS Certificate	Determines the certificate used for authentication: <ul style="list-style-type: none"> • Manufacturing issued • User installed 	Installing Authentication Certificates for EAP-TLS Authentication, page 4-17
Validate Server Certificate	Enables the phone to use the server certificate. Two options: true or false. Note Applies to PEAP only.	

Table 4-3 Basic Network Profile Settings (continued)

Item	Description	For More Information, See...
IP Network Configuration		
Obtain IP address and DNS servers automatically	Gets the IP address and DNS servers automatically.	Configuring IP Network Settings, page 4-23
Use the following IP address and DNS servers	Disables DHCP and uses these static settings: <ul style="list-style-type: none"> • IP Address • Subnet Mask • Default Router • Primary DNS • Secondary DNS • Domain Name 	
TFTP		
Obtain TFTP Servers Automatically	Enables automatic assignment of TFTP servers	Configuring the Alternate TFTP Server, page 4-24
Use the following TFTP servers	Assigns static TFTP server IP addresses to: <ul style="list-style-type: none"> • TFTP Server 1 • TFTP Server 2 	

Table 4-4 Advanced Network Profile Settings

TSPEC Settings		
Minimum PHY Rate	Minimum data rate that outbound traffic uses. Modify this setting when Call Admission Control (CAC) is enabled. Note Cisco APs support only PHY rates of 6, 11, 12, or 24. The default is 12. If you use an access point that using 802.11b, the PHY rate must be configured to the supported rate.	Configuring Advanced Network Profile Settings, page 4-25
Surplus Bandwidth	Excess bandwidth beyond application requirements	
802.11G Power Settings		
Channel	Assigns the channels	Configuring Advanced Network Profile Settings, page 4-25
Status	Enabled—Identifies enabled channels in WLAN to improve scanning for the phone.	
MaxTxPower	Sets the maximum transmit power for the phone	

Table 4-4 *Advanced Network Profile Settings (continued)*

802.11A Power Settings		
Channel	Assigns the channels	Configuring Advanced Network Profile Settings, page 4-25
Status	Enabled—Identifies enabled channels in WLAN to improve scanning for the phone	
Max Tx Power	Sets the maximum transmit power for the phone	

**Note**

If you uncheck all channels in the 802.11g Power Settings window or 802.11a Power Settings window, the phone will not be able to access the WLAN.

Related Topics

- [Accessing the Phone Web Page, page 4-3](#)
- [Configuring Wireless LAN Security, page 4-13](#)
- [Setting the Wireless Security Credentials, page 4-15](#)
- [Setting Wireless Encryption, page 4-16](#)

Configuring Wireless Settings in a Network Profile

You must configure wireless settings in a profile to enable the phone to access the wireless network. To configure the wireless settings, refer to [Table 4-3](#) and follow these steps.

Procedure

-
- Step 1** Choose the network profile that you want to configure.
- Step 2** To give the profile a recognizable name, in the Profile Name field, enter a name up to 63 characters and numbers in length.
- Step 3** To identify the SSID that the phone uses to associate with access points, in the SSID field, enter an SSID that is already configured in the WLAN.

**Note**

The SSID is case sensitive; you must enter it exactly as configured in the network.

- Step 4** To conserve battery power, in the Call Power Save Mode, choose the type (U-APSD or PS-Poll) and option that is being used in the WLAN.
- Step 5** Choose the signal mode or priority of signal modes in the 802.11 Mode field that is used by your WLAN,
-

Configuring Wireless LAN Security

The Cisco Unified Wireless IP Phone 7925G supports many types of authentication. Authentication methods might require a specific encryption method or you can choose between several encryption methods. When configuring a network profile, you can choose one of these authentication methods:

- Open—Provides access to all access points without WEP Key authentication/encryption.
- Open plus WEP—Provides access to all access points and authentication through the use of one or more WEP Keys at the local access point.
- Shared Key plus WEP—Provides shared key authentication through the use of WEP Keys at the local access point.
- LEAP—Exchanges a username and cryptographically secure password with a RADIUS server for authentication in the network. LEAP is a Cisco proprietary version of EAP.
- EAP-FAST—Exchanges a username and password and with a RADIUS server for authentication in the network.
- EAP-TLS—Uses a dynamic session-based WEP key derived from the client adapter and RADIUS server to encrypt data and a client certificate for authentication. It uses PKI to secure communication to the RADIUS authentication server.
- PEAP (EAP-MSCHAP V2)—Performs mutual authentication, but does not require a client certificate on the phone. This method uses name and password authentication based on Microsoft MSCHAP V2 authentication.
- PEAP with Server Certificate Authentication—The Cisco Unified Wireless IP Phone 7925G can validate the server certificate during the authentication handshakes over an 802.11 wireless link. This functionality is disabled by default and is enabled in Cisco Unified Communications Manager Administration.
- Auto (AKM)—Automatic authenticated key management in which the phone selects the AP and type of key management scheme, which includes WPA, WPA2, WPA-Pre-shared key, WPA2-Pre-shared key, or CCKM (which uses a wireless domain server (WDS)).



Note

When set to AKM mode, the phone uses LEAP for 802.1x type authentication methods (non-Pre-shared key such as WPA, WPA2, or CCKM). AKM mode supports only authenticated key-management types (WPA, WPA2, WPA-PSK, WPA2-PSK, CCKM).

The type of authentication and encryption schemes that you are using with your WLAN determine how you set up the authentication, security, and encryption options in the network profiles for the Cisco Unified Wireless IP Phones. [Table 4-5](#) provides a list of supported authentication and encryption schemes that you can configure on the Cisco Unified Wireless IP Phone 7925G.

Table 4-5 Authentication and Encryption Configuration Options

Authentication Mode	Wireless Encryption	Wireless Security Credentials
Open	None	None—access to all APs
Open plus WEP	Static WEP Requires WEP Key	None—access to all APs
Shared Key plus WEP	Static WEP Requires WEP Key	Uses shared-key with AP

Table 4-5 Authentication and Encryption Configuration Options (continued)

Authentication Mode	Wireless Encryption	Wireless Security Credentials
LEAP (with optional CCKM)	Uses WEP	Requires Username and Password
EAP-FAST (with optional CCKM)	Uses WEP or TKIP	Requires Username and Password
EAP-TLS	Uses WEP, TKIP, or AES	Requires Username and Password Requires server and client certificates.
PEAP	Uses WEP, TKIP, or AES	Requires Username and Password Requires server side certificate.
Auto (AKM) with CCKM	Uses TKIP or AES	Requires Username and Password
Auto (AKM) with WPA (with optional CCKM)	Uses TKIP	Requires Username and Password
Auto (AKM) with WPA2 (with optional CCKM)	Uses AES	Requires Username and Password
Auto (AKM) with WPA Pre-Shared Key	Uses TKIP	Requires Passphrase
Auto (AKM) with WPA2 Pre-Shared Key	Uses AES	Requires Passphrase

**Note**

Beginning with Cisco Wireless IP Phone 7925G firmware release 1.1, CCKM is operational with the WPA authentication mode using AES encryption.

Configuring the Authentication Mode

To select the Authentication Mode for this profile, follow these steps:

Procedure

-
- Step 1** Choose the network profile that you want to configure.
- Step 2** Choose the authentication mode.



Note Depending on what you selected, you must configure additional options in Wireless Security or Wireless Encryption. See [Table 4-5](#) for more information.

- Step 3** Click **Save** to make the change.
-

Setting the Wireless Security Credentials

When your network uses EAP-FAST, LEAP, EAP-TLS, PEAP, or Auto (AKM) with WPA, WPA2, CCKM for user authentication, you must configure both the username and a password on the Access Control Server (ACS) and the phone.

**Note**

If you use domains within your network, you must enter the username with the domain name, in this format: *domain\username*.

For information about setting security credentials, see these topics:

- [Configuring the Username and Password, page 4-15](#)
- [Configuring the Pre-shared Key, page 4-15](#)
- [Setting Wireless Encryption, page 4-16](#)
- [Installing Authentication Certificates for EAP-TLS Authentication, page 4-17](#)
- [Configuring PEAP, page 4-22](#)

Configuring the Username and Password

To enter or change the username or password for the network profile, you must use the same username and the same password string that is configured in the RADIUS server. The maximum length of the username or password entry is 32 characters.

To set up the username and password in Wireless Security Credentials, follow these steps:

Procedure

- Step 1** Choose the network profile.
- Step 2** In the Username field, enter the network username for this profile.
- Step 3** In the Password field, enter the network password string for this profile.
- Step 4** Click **Save** to make the change.

Configuring the Pre-shared Key

When using Auto (AKM) with WPA Pre-shared key or WPA2 with Pre-shared key for authentication, you must configure a Passphrase/Pre-shared key in the Wireless Security Credentials area.

Pre-shared Key Formats

The Cisco Unified Wireless IP Phone 7925G supports ASCII and hexadecimal formats. You must use one of these formats when setting up a WPA Pre-shared key:

Hexadecimal

For hexadecimal keys, you must enter 64 hex digits (0-9 and/or A-F); for example, AB123456789CD01234567890EFAB123456789CD01234567890EF3456789C

ASCII

For ASCII keys, you must enter a character string that uses 0-9, A-Z (upper and lower case), including symbols and is from 8 to 63 characters in length; for example, GREG12356789ZXZYW

To set up a Pre-shared key in the Wireless Credentials area, follow these steps:

Procedure

-
- Step 1** Choose the network profile that uses Auto (AKM) to enable the WPA Pre-shared key or WPA2 Pre-shared key.
- Step 2** In the Key Type area, choose one of these character formats:
- **Hex**
 - **ASCII**
- Step 3** Enter an ASCII string or Hex digits in the Passphrase/Pre-shared key field. See [“Pre-shared Key Formats” section on page 4-15](#).
- Step 4** Click **Save** to make the change.
-

Setting Wireless Encryption

If your wireless network uses WEP encryption, and you have set the Authentication Mode as Open + WEP or Shared Key + WEP, you must enter an ASCII or hexadecimal WEP Key.

The WEP Keys for the phone must match the WEP Keys assigned to the access point. Cisco Unified Wireless IP Phone 7925G and Cisco Aironet Access Points support both 40-bit and 128-bit encryption keys.

WEP Key Formats

You must use one of these formats when setting up a WEP key:

Hexadecimal

For hexadecimal keys, you can use one of the following key sizes:

- 40-bit—You must enter a 10-digit encryption key string that uses the hex digits (0-9 and/or A-F); or example, ABCD123456.
- 128-bit—You must enter a 26-digit encryption key string that uses the hex digits (0-9 and/or A-F); or example, AB123456789CD01234567890EF.

ASCII

For ASCII keys, you must enter a character string that uses 0-9, A-Z (upper and lower case), and all symbols.

- 40-bit—You must enter a 5-character string; for example, GREG5.
- 128-bit—You must enter a 13-character string; for example, GREGSSECRET13.

Entering Wireless Encryption Keys

To set up WEP keys, follow these steps:

Procedure

- Step 1** Choose the network profile that uses Open+WEP or Shared+WEP.
- Step 2** In the Key Type area, choose one of these character formats:
- Hex
 - ASCII
- Step 3** For Encryption Key 1, click **Transmit Key**.
- Step 4** In the Key Size area, choose one of these character string lengths:
- 40
 - 128
- Step 5** In the Encryption Key field, enter the appropriate key string based on the selected Key Type and Key Size. See the “WEP Key Formats” section on page 4-16.
- Step 6** Click **Save** to make the change.
-

Related Topics

- [Configuring IP Network Settings, page 4-23](#)
- [Configuring the Alternate TFTP Server, page 4-24](#)
- [Configuring Advanced Network Profile Settings, page 4-25](#)

Installing Authentication Certificates for EAP-TLS Authentication

EAP-TLS is a certificate based authentication that requires a trust relationship between two or more entities. Each entity has a certificate proving its identity and is signed by a trusted authority. These certificates are exchanged and verified during EAP-TLS authentication.



Note

The EAP-TLS certificate based authentication requires that the internal clock on the Cisco Unified Wireless IP Phone 7925G be set correctly. Use the phone web page to set the clock on the phone before using EAP-TLS authentication.

To use EAP-TLS, both the Cisco Unified Wireless IP Phone 7925G and the Cisco Secure Access Control Server (ACS) must have certificates installed and configured properly. If your wireless network uses EAP-TLS for authentication, you can use the Manufacturing Installed Certificate (MIC) or a user installed certificate for authentication on the phone.

Manufacturing Installed Certificate

Cisco has included a Manufacturing Installed Certificate (MIC) in the phone at the factory.

During EAP-TLS authentication the ACS server needs to verify the trust of the phone and the phone needs to verify the trust of the ACS server.

To verify the MIC, the Manufacturing Root Certificate and Manufacturing Certificate Authority (CA) Certificate must be exported from a Cisco Unified Wireless IP Phone 7925G and installed on the Cisco ACS server. These two certificates are part of the trusted certificate chain used to verify the MIC by the Cisco ACS server.

To verify the Cisco ACS certificate, a trusted subordinate certificate (if any) and root certificate (created from a CA) on the Cisco ACS server must be exported and installed on the phone. These certificate(s) are part of the trusted certificate chain used to verify the trust of the certificate from the ACS server.

User Installed Certificate

To use a user installed certificate, a Certificate Signing Request (CSR) must be generated on the phone, sent to the CA for approval, and the approved certificate installed on the Cisco Unified Wireless IP Phone 7925G.

During EAP-TLS authentication, the ACS server needs to verify the trust of the phone and the phone needs to verify the trust of the ACS server.

To verify the authenticity of the user installed certificate, a trusted subordinate certificate (if any) and root certificate from the CA that approved the user certificate must be installed on the Cisco ACS server. These certificate(s) are part of the trusted certificate chain used to verify the trust of the user installed certificate.

To verify the Cisco ACS certificate, a trusted subordinate certificate (if any) and root certificate (created from a CA) on the Cisco ACS server must be exported and installed on the phone. These certificate(s) are part of the trusted certificate chain used to verify the trust of the certificate from the ACS server.

To install authentication certificates for EAP-TLS, perform the tasks listed in [Table 4-6](#):

Table 4-6 *Installing the Certificate for EAP-TLS*

Task	From	For more information, see...
1. Set the Cisco Unified Communications Manager date and time on the phone.	Cisco Unified Wireless IP Phone 7925G web page	Setting the Date and Time, page 4-19
2. If using the Manufacturing Installed Certificate (MIC): <ol style="list-style-type: none"> a. Export the CA root certificate and manufacturing CA certificate. b. Install certificates on the Cisco ACS server and edit the trust list. c. Export the CA certificate from the ACS server and import it to the phone. 	<ul style="list-style-type: none"> • Cisco Unified Wireless IP Phone 7925G web page • Internet Explorer • Microsoft Certificate Services 	Exporting and Installing the Certificates on the ACS, page 4-19 Exporting the CA Certificate from the ACS Using Microsoft Certificate Services, page 4-20

Table 4-6 Installing the Certificate for EAP-TLS (continued)

Task	From	For more information, see...
3. If using a user installed certificate: <ol style="list-style-type: none"> a. Generate the Certificate Signing Request (CSR). b. Send the CSR to CA to sign. c. Import the certificate. d. Install certificate on the Cisco ACS server and edit the trust list. e. Download the CA certificate from the ACS server and import it into the 7925G. 	Cisco Unified Wireless IP Phone 7925G web page	Requesting and Importing the User Installed Certificate, page 4-21
4. Set up the user account.	ACS configuration tool	Configuring the ACS Server Setup, page 4-22 <i>User Guide for Cisco Secure ACS for Windows</i>

Setting the Date and Time

EAP-TLS uses certificate based authentication that requires the internal clock on the Cisco Unified Wireless IP Phone 7925G to be set correctly. The date and time on the phone might change when it is registered to Cisco Unified Communications Manager.



Note

If a new server authentication certificate is being requested and the local time is behind the Greenwich Mean Time (GMT), the authentication certificate validation might fail. It is recommended that you set the local date and time ahead of the GMT.

To set the phone to the correct local date and time, follow these steps:

Procedure

-
- Step 1** Select **Date & Time** from the left navigation pane.
 - Step 2** If the setting in the Current Phone Date & Time field is different from the Local Date & Time field, click **Set Phone to Local Date & Time**.
 - Step 3** Click **Phone Restart**, then click **OK**.
-

Exporting and Installing the Certificates on the ACS

To use the MIC, the Manufacturing Root Certificate and Manufacturing CA Certificate must be exported and installed onto the Cisco ACS server.

To export the manufacturing root certificate and manufacturing CA certificate to the ACS server, follow these steps:

Procedure

-
- Step 1** From the phone web page, choose Certificates. Click Export next to the Manufacturing Root Certificate.
- Step 2** Save the certificate and copy it to the ACS server.
- Step 3** Repeat Steps 1 and 2 for the Manufacturing CA certificate.
- Step 4** From the ACS Server System Configuration page, enter the file path for each certificate and install the certificates.



Note For more information about using the ACS configuration tool, see the ACS online help or the *User Guide for Cisco Secure ACS for Windows*.

- Step 5** Use the Edit the Certificate Trust List (CTL) page to add the certificates to be trusted by ACS.
-

Exporting Certificates from the ACS

Depending on the type of certificate you export from the ACS, use one of the following methods:

- To export the CA certificate from the ACS server that signed the user installed certificate or ACS certificate, see [Exporting the CA Certificate from the ACS Using Microsoft Certificate Services, page 4-20](#).
- To export the CA certificate from the ACS server that uses a self-signed certificate, see [Exporting Certificates from the ACS Server Using Internet Explorer, page 4-20](#).

Exporting the CA Certificate from the ACS Using Microsoft Certificate Services

Use this method for exporting the CA certificate from the ACS server that signed the user installed certificate or ACS certificate.

To export the CA certificate using the Microsoft Certificate Services web page, follow these steps:

Procedure

-
- Step 1** From the Microsoft Certificate Services web page, select Download a CA certificate, certificate chain or CRL.
- Step 2** At the next page, highlight the current CA certificate in the text box, choose DER under Encoding Method, then click Download CA certificate.
- Step 3** Save the CA certificate.
-

Exporting Certificates from the ACS Server Using Internet Explorer

Use this method for exporting the CA certificate from the ACS server that uses a self-signed certificate.

To export certificates from the ACS server using Internet Explorer, follow these steps:

Procedure

-
- Step 1** From Internet Explorer, choose Tools > Internet Options, then click the Content tab.

- Step 2** Under Certificates, click **Certificates...**, then click the Trusted Root Certification Authorities tab.
 - Step 3** Highlight the root certificate and click **Export...** The Certificate Export Wizard appears. Click **Next**.
 - Step 4** At the next window, select **DER encoded binary X.509 (.CER)**, and click **Next**.
 - Step 5** Specify a name for the certificate and click **Next**.
 - Step 6** Save the CA certificate to be installed on the phone.
-

Requesting and Importing the User Installed Certificate

To request and install the certificate on the phone, follow these steps:

Procedure

- Step 1** From the phone web page, choose the network profile using EAP-TLS, and select **User Installed** in the EAP-TLS Certificate field.
 - Step 2** Click **Certificates**. On the User Certificate Installation page, the Common Name field should match the user name in the ACS server.
Note You can edit the Common Name field if you wish. Make sure that it matches the user name in the ACS server. See [“Configuring the ACS Server Setup”](#) section on page 4-22.

Enter the information to be displayed on the certificate, and click **Submit** to generate the Certificate Signing Request (CSR).
 - Step 3** In the next screen, select and copy the entire contents of the text box. Send this data to the CA administrator for signing.

The CSR text is encoded and should be sent to the Certificate Authority for signing. The CSR text can be sent by e-mail or another method determined by your CA administrator. The following steps describe the basic CSR approval process on the CA web page.
 - Step 4** From the Microsoft Certificate Services Request a Certificate page, select **Advanced certificate request** to initiate the signing request.
 - Step 5** At the Advanced Certificate Request page, select **Submit a certificate request by using a base-64-encoded PKCS CMC**.
 - Step 6** Copy the certificate data from the Cisco Unified Wireless IP Phone 7925G and paste it in the Saved Request text box, then click **Submit**.
 - Step 7** Once the CSR is approved, the certificate must be exported in a DER encoded format and sent to the original requestor.
 - Step 8** Return to the phone web page and choose **Certificates** to import the signed certificate.
 - Step 9** On the Certificates page, locate the User Installed certificate line, and click **Import**. Browse to the certificate on your PC to import to the phone.
-

Installing the Authentication Server Root Certificate

The Authentication Server Root Certificate must be installed on the Cisco Unified Wireless IP Phone 7925G.

To install the certificate, follow these steps:

-
- Step 1** Export the Authentication Server Root Certificate from the ACS. See [Exporting Certificates from the ACS, page 4-20](#).
- Step 2** Go to the phone web page and choose **Certificates**.
- Step 3** Click **Import** next to the Authentication Server Root certificate.
- Step 4** Restart the phone.
-

Configuring the ACS Server Setup

To set up the user account name and install the MIC root certificate for the phone on the ACS, follow these steps:



Note For more information about using the ACS configuration tool, see the ACS online help or the *User Guide for Cisco Secure ACS for Windows*.

Procedure

-
- Step 1** From the ACS configuration tool User Setup page, create a phone user account name if it is not already set up. Typically, the user name includes the phone MAC address at the end (for example, CP-7925G-SEPxxxxxxxxxxxx). No password is necessary for EAP-TLS.
- Note** Make sure the user name matches the Common Name field in the User Certificate Installation page. See [“Requesting and Importing the User Installed Certificate” section on page 4-21](#).
- Step 2** On the System Configuration page, in the EAP-TLS section, enable these fields:
- Allow EAP-TLS
 - Certificate CN comparison.
- Step 3** On the ACS Certification Authority Setup page, add the Manufacturing Root Certificate and Manufacturing CA Certificate to the ACS server.
- Step 4** Enable both the Manufacturing Root Certificate and Manufacturing CA Certificate in the ACS Certificate Trust List.
-

Configuring PEAP

Protected Extensible Authentication Protocol (PEAP) uses server-side public key certificates to authenticate clients by creating an encrypted SSL/TLS tunnel between the client and the authentication server.



Note The authentication server validation can be enabled by importing the authentication server certificate.

Before You Begin

Before you configure PEAP authentication for the phone, make sure these Cisco Secure ACS requirements are met:

- The ACS root certificate must be installed
- Enable the Allow EAP-MSCHAPv2 setting
- User account and password must be configured
- For password authentication, you can use the local ACS database or an external one (such as Windows or LDAP)

Enabling PEAP Authentication

To enable PEAP authentication on the phone, follow these steps:

Procedure

-
- Step 1** From the phone configuration web page, choose PEAP as the authentication mode. See [Configuring the Authentication Mode, page 4-14](#).
- Step 2** Enter a user name and password.
-

Configuring IP Network Settings

The Cisco Unified IP Phones enable DHCP, by default, to automatically assign IP addresses to devices when you connect them to the network. If you do not use DHCP in your network, then you must disable DHCP and manually enter network configuration information. For more information, see [“Interacting with the Dynamic Host Configuration Protocol Server” section on page 2-15](#).

When DHCP is disabled in the network, you must configure the following settings in the Static Settings menu:

- IP address
- Subnet mask
- Default Router
- DNS server 1 and 2
- TFTP server 1

Use these guidelines when manually configuring the IP settings:

- Ensure the TFTP server has an IP address.
- Ensure the default router IP address is on the same subnet as the host IP address.

Enabling DHCP

To enable the use of DHCP in the Network Profile, follow these steps:

Procedure

-
- Step 1** Choose the network profile that you want to configure.
- Step 2** Under the IP Network Configuration area, choose this option:
Obtain IP address and DNS servers automatically

Step 3 Click **Save** to make the change.

Disabling DHCP

To disable the use of DHCP in the Network Profile, follow these steps:

Procedure

- Step 1** Choose the network profile that you want to configure.
- Step 2** Under the IP Network Configuration area, choose this option:
Use the following IP addresses and DNS servers
- Step 3** You must enter these required IP addresses. See [Table 4-7](#) for descriptions of these fields.
- Step 4** Click **Save** to make the change.
-

Table 4-7 *Static IP Addresses When DHCP is Disabled*

Static Setting	Description
IP Address	IP address of the phone
Subnet Mask	Subnet mask used by the phone
Default Router 1	Primary gateway used by the phone
DNS Server 1	Primary DNS server used by the phone
DNS Server 2	Optional backup DNS server used by the phone
TFTP Server 1	Primary TFTP server used by the phone
TFTP Server 2	Optional backup TFTP server used by the phone
Domain Name	Name of the DNS in which the phone resides

Configuring the Alternate TFTP Server

If you use DHCP to direct the Cisco Unified Wireless IP Phone 7925Gs to a TFTP server, you can also assign an alternative TFTP server to some phones instead of the one assigned by DHCP.



Note If you disable DHCP, then you must use these steps to set up the TFTP server for the phone.

To assign an alternate TFTP server to a phone, follow these steps:

Procedure

- Step 1** Choose the network profile that you want to configure.
- Step 2** In the TFTP area, choose this option:
Use the following TFTP servers

- Step 3** You must enter the required IP addresses. See [Table 4-7](#) for descriptions of these fields.
- Step 4** Click **Save** to make the change.
-

Configuring Advanced Network Profile Settings

The Network Profiles in the Settings menu enable the settings for QoS, bandwidth, and power. The Traffic Specification (TSPEC) parameters are used to advertise information about generated traffic for Call Admission Control (CAC) to the AP. The parameters are:

- Minimum PHY rate—Lowest rate that outbound traffic is expected to use before the phone roams to another AP
- Surplus Bandwidth Allowance—Fractional number that specifies the excess allocation of time and bandwidth above application rates required to transport a MAC service data unit (MSDU) in a TSPEC frame.

**Note**

If your wireless LAN has access points that use 802.11b and you plan to use Call Admission Control (CAC) with TSPEC, then you need to modify the PHY rate to a supported rate for your 802.11b access points.

To make changes to the advanced settings, follow these steps:

Procedure

- Step 1** Choose the network profile that you want to configure.
- Step 2** Click the Advanced Profile link at the top of the page.
- Step 3** In the TSPEC Setting area, it is recommended that you keep the minimum PHY rate at 12 Mbps.

**Note**

If you are using 802.11b APs and plan to use Call Admission Control (CAC) with TSPEC, then set the PHY Rate to a rate that the APs support such as 11 Mbps.

- Step 4** In the Surplus Bandwidth field, enter the appropriate values.
- Step 5** In the 802.11G Power Settings area, check only the channels that are used in your WLAN. By doing this, the phone scans for only those channels.
In the Max Tx Power field, keep the default value.
- Step 6** In the 802.11A Power Settings area, check only the channels that are used in your WLAN. By doing this, the phone scans for only those channels.
In the Max Tx Power field, keep the default value.

**Caution**

You must check at least one channel after using “Clear All,” to enable the phone to access the WLAN.

- Step 7** Click **Save** to make the change.
-

Related Topics

- [Accessing the Configuration Web Page for a Phone, page 4-5](#)
- [Network Profile Settings, page 4-8](#)
- [Configuring Wireless Settings in a Network Profile, page 4-12](#)
- [Configuring Wireless LAN Security, page 4-13](#)
- [Setting the Wireless Security Credentials, page 4-15](#)
- [Configuring the Pre-shared Key, page 4-15](#)
- [Configuring IP Network Settings, page 4-23](#)
- [Configuring the Alternate TFTP Server, page 4-24](#)

Configuring USB Settings

To use the USB cable from your PC to a phone, you must configure the USB settings to work with the USB port on the PC. The phone has a default USB IP address of 192.168.1.100. You can change the USB port configuration on the phone in these ways:

- To obtain the IP address automatically, by getting an IP address from the PC that has DHCP set up.
- To use the IP address and subnet mask assigned in this area.

To display the USB Settings area, access the web page for the phone as described in the “[Accessing the Phone Web Page](#)” section on [page 4-3](#), and then click the **USB Settings** hyperlink.

To change the USB port settings for the phone, follow these steps:

Procedure

-
- | | |
|---------------|---|
| Step 1 | On the phone web page, choose the USB Settings hyperlink. |
| Step 2 | Choose one of the following options: <ul style="list-style-type: none">• Obtain IP address automatically• Use the following IP address |
| Step 3 | To change the static IP address, in the IP Address field, enter a new IP address that is not assigned on the subnet. |
| Step 4 | To change the subnet for the new IP address, in the Subnet Mask field, enter the appropriate subnet address. |
| Step 5 | Click Save to make the change. |
-

Related Topics

- [Accessing the Phone Web Page, page 4-3](#)
- [Configuring Network Profiles, page 4-8](#)
- [Configuring Trace Settings, page 4-27](#)
- [Using System Settings, page 4-34](#)

Configuring Trace Settings

You can use the Trace Settings area on the web page to configure how the phone creates and saves trace files. Because trace files are stored in the memory of the phone, you can control the number of files and the data that you want to collect. [Table 4-8](#) describes these configurable items.

**Note**

When preserving trace logs, choose only the logs that need to be saved after the phone is powered off and powered on to avoid using up phone memory.

To display the Trace Settings area, access the web page for the phone as described in the “[Accessing the Phone Web Page](#)” section on page 4-3, and then click the **Trace Settings** hyperlink under Setup.

To change the trace settings for the phone, follow these steps:

Procedure

-
- Step 1** On the phone web page, choose the Trace Settings hyperlink.
- Step 2** In the Number of Files field, choose the number of trace files to save, from 2 to 10.
- Step 3** In the Remote Syslog Server area, check the box to enable a server to collect the trace files.
- Step 4** If you enabled the syslog server, then you must complete these fields:
- IP Address—Enter server IP address
 - Port—Enter a port number (514, 1024-65535)
- Step 5** In the Module Trace Level area, check only the modules for which you want data:
- Kernel
 - Wireless LAN Driver
 - Wireless LAN Manager
 - Configuration
 - Call Control
 - Network Services
 - Security Subsystem
 - User Interface
 - Audio System
 - System
- Step 6** In the Advanced Trace Settings area, in the Preserve Logs field, choose one of the following:
- True—Save the trace logs to flash memory on the phone.
 - False—Save the trace logs to RAM.

**Note**

-
- When set to False, the trace logs are lost when the phone is powered off.
 - When the phone is powered off, then powered back on, the Preserve Logs field is reset to False, the default value.
-

Step 7 Click **Save** to make the change.

Table 4-8 Trace Settings Area Items

Item	Description
General	
Number of Files	Choose the number of trace files that the phone saves, from 2-10 files.
File Size	Choose the File size for the trace file that is saved. The file size range is 50K to 250K.
Remote Syslog Server	
Enable Remote Syslog	Set up a remote server to store trace logs IP Address—Enter server IP address Port—Enter a port number (514, 1024-65535)
Module Trace Level	
Kernel	Operating System data
Wireless LAN Driver	Channel scanning and authentication
Wireless LAN Manager	Channel scanning and authentication
Configuration	Phone configuration data
Call Control	Cisco Unified Communications Manager data
Network Services	DHCP, TFTP, CDP data
Security Subsystem	Application level security data
User Interface	Key strokes, softkeys, MMI data
Wireless	Channel scanning, authentication data
Audio System	RTP, SRTP, RTCP, DSP data
System	Firmware, upgrade data
Advanced Trace Settings	
Preserve Logs	True—Save trace logs after powering off the phone False—Delete trace logs
Reset Trace Settings upon Reboot	You may enable debugging by configuring various settings on the Trace Configuration. These options determine how trace settings are handled when you reboot: <ul style="list-style-type: none"> • Yes—Default value. Settings will be reset to the default values upon reboot. • No—Trace settings will not reset upon reboot.

Related Topics

- [Accessing the Phone Web Page, page 4-3](#)
- [Configuring Network Profiles, page 4-8](#)
- [Configuring USB Settings, page 4-26](#)
- [Using System Settings, page 4-34](#)

Configuring Wavelink Settings

The Cisco Unified Wireless IP Phone 7925G supports the use of the Wavelink Avalanche server to configure the phone, which can be set up as a Wavelink Avalanche client device. The Cisco Unified Wireless IP Phone 7925 Configuration Utility can be installed on the Wavelink Avalanche server to configure a single phone or multiple phones with common settings. For more information, see [Chapter 6, “Configuring the Phone Using the Wavelink Avalanche Server.”](#)

You can use the phone web page to assign attributes to the phone that can be used to distinguish it from other mobile devices connected to the Wavelink server. These attributes can be used as search criteria for locating phones on the Wavelink server. For example, the predefined ModelName parameter with a value of “CP7925G” will identify a device as the Cisco Unified Wireless IP Phone7925G.

By default, the following parameters are configured as follows:

- ModelName = CP7925
- EnablerVer = 3.11-01

To configure Wavelink parameters using the phone web page, follow these steps:

Procedure

-
- Step 1** From the phone web page, choose **Wavelink Settings**.
- Step 2** In the Wavelink Custom Parameters section, enter values for each parameter in the Name and Value fields. You can define up to four pairs of custom parameters.



Note Do not use spaces in the Name field.



Note For more information about using the Wavelink Avalanche server, see [Assigning the Wavelink Server, page 6-2](#).

Configuring the Phone Book

Cisco Unified Wireless IP Phone 7925G users can store up to 100 contacts in the Phone Book on the phone. As the administrator, you can configure the Phone Book for these phones from the phone web page.



Note Before you can access the Phone Book from the phone web page, you must enable the Phone Book Web Access privilege in Cisco Unified Communications Manager Administration. For more information, see [Setting Configuration Privileges for the Phone Web Page, page 4-4](#).

You can perform the following tasks for the Phone Book:

- Import or export a file from/to the Phone Book—See [Importing and Exporting Contacts, page 4-30](#)
- Import or export Microsoft Outlook Contacts—See [Importing and Exporting CSV Phone Contact Records, page 4-30](#)

- Search the Phone Book for a contact—See [Searching the Phone Book Information, page 4-32](#)
- Update the Phone Book contact information—See [Updating Phone Book Information, page 4-32](#)
- Assign a speed dial to contact phone number—See [Assigning A Speed-Dial Hot Key to a Contact Number, page 4-33](#)

Importing and Exporting Contacts

To import contact information from a file, follow these steps:

Procedure

-
- Step 1** From the phone web page, choose **Phone Book > Import/Export** from the left pane.
- Step 2** At the Phone Book Import & Export page, do one of the following:
- To import a file, browse to it on your PC. Choose one of the following options, then click **Import**:
 - Delete all current contacts before importing
 - Delete only the current contacts that have the same IDs
 - Merge current contacts with imported data
 - To export a file, click **Export**. A file with your contact information is displayed. Save this file to your PC or another storage device.
-

Importing and Exporting CSV Phone Contact Records

To export or import phone contact records using the Comma Separated Values (CSV) format enables the viewing, editing, or creating records with third party software such as Microsoft Excel and Microsoft Outlook. After editing or creating records, the records can transferred to the Cisco Unified Wireless IP Phone 7925G.



Note

The Cisco Unified Wireless IP Phone 7920G CSV files can be imported into the Cisco Unifies Wireless IP Phone7925G.

Each records contains fields separated by commas. The supported field names are as follows:

- First Name
- Last Name
- Company
- Business Street
- Business City
- Business State
- Business Postal Code
- Business Country
- Home Phone

- Home Speed Dial
- Business Phone
- Business Speed Dial
- Mobile Phone
- Mobile Speed Dial
- Business Fax
- Fax Speed Dial
- Other Phone
- Other Speed Dial (Speed Dial for Other/FAX Phone)
- Primary Phone (must match one of above phone numbers)
- E-mail Address

The following field names generated by the Cisco Unified Wireless IP Phone 7925G do not map to Microsoft Outlook by default:

- Nickname
- IM Address
- Unique Identifier (UUID)

Since the importing file may not have the UUID field generated by the Cisco Unified Wireless IP Phone 7925G, the import procedure includes the option for the user to use name fields as a way to match the importing record with the existing phone book records on the phone. Deleting or merging matching records is supported.

The first-name last-name fields must be matched with the following criteria:

- Use the First-Name and Last-Name to match if one of them is valid.
- Use the Company-Name field if other name fields are empty.

Microsoft Outlook 2003 does not support exporting or importing of Unicode characters. Since Microsoft Outlook 2003 uses the native international language characters when displaying the contacts list, it does not export these characters in the CSV file format. The Cisco Unified Wireless IP Phone 7925G uses the UTF-8 to encode the international character sets and Microsoft Outlook 2003 can import or export these characters; however, Microsoft Outlook 2003 may not properly display these characters.

Perform the following steps to import or export the phone book records into a file using CSV format.

Procedure

-
- Step 1** Access the web interface of the Cisco Unified Wireless IP Phone 7925G.
- Step 2** Select the PHONE BOOK menu.
- Step 3** To import, click the Import option. Specify how old and duplicated contact records are processed. Click the Create File of Type:.
- Step 4** Click the Comma Separated Values (CSV) format.
- Step 5** To export, click the Export option.
- Note** If a Security Alert window displays, click Yes.
- Step 6** Click Open, Save, or Cancel displays. Click Save and specify the filename and location. Then click Save again.

- Step 7** Click Import when all options had been specified.
- Step 8** Check the Status web page because it displays the number of valid records that were processed. Since the import function duplicates UIDs and names, the total number of created contacts on the phone may be less than the total number of records processed.
-

Searching the Phone Book Information

You can search for contacts in the Phone Book by first name, last name, nickname, or company name. To perform a search, follow these steps:

Procedure

- Step 1** From the phone web page, choose **Phone Book** from the left pane.
- Step 2** At the Phone Book page, enter a search string in the text box and click **Search**.
The contact records containing a match will be displayed.
-

Updating Phone Book Information

You can update the information for Phone Book from the phone web page. You can perform the following tasks:

- Add a contact—See [Adding a Contact, page 4-32](#)
- Delete contacts—See [Deleting Contacts, page 4-33](#)
- Edit the information for a contact—See [Editing Contact Information, page 4-33](#)



Note

When entering phone numbers, only numeric characters and the symbols # and * are stored and displayed.

Adding a Contact

To add a contact to the Phone Book, follow these steps:

Procedure

- Step 1** From the phone web page, choose **Phone Book** from the left pane.
- Step 2** At the Phone Book page, click New. The Phone Book (New Contact) page appears.
- Step 3** Enter information for this contact. If you wish to assign speed dials, see [Assigning A Speed-Dial Hot Key to a Contact Number, page 4-33](#).
- Step 4** When finished, click **Save**.
-

Deleting Contacts

To delete contacts from the Phone Book, follow these steps:

Procedure

- Step 1** From the phone web page, choose **Phone Book** from the left pane.
 - Step 2** At the Phone Book page, select the contacts to delete, and click **Delete**.
To delete all contacts, click **DeleteAll**.
-

Editing Contact Information

To edit information for a contact, follow these steps:

Procedure

- Step 1** From the phone web page, choose **Phone Book** from the left pane.
 - Step 2** At the Phone Book page, select a contact. The Phone Book (Edit Contact) page appears.
 - Step 3** Change or enter information for this contact. If you wish to assign speed dials, see [Assigning A Speed-Dial Hot Key to a Contact Number](#), page 4-33.
 - Step 4** When finished, click **Save**.
-

Assigning A Speed-Dial Hot Key to a Contact Number

You can assign a speed-dial hot key to any contact phone number in the Phone Book.

To assign a speed-dial hot key to a contact number, follow these steps:

Procedure

- Step 1** From the phone web page, add a new contact or select a contact record to edit. For more information, see [Adding a Contact](#), page 4-32 or [Editing Contact Information](#), page 4-33.
 - Step 2** At the Phone Book (Edit Contact) page or the Phone Book (New Contact) page, click the speed dial icon next to the phone number you wish to assign.
 - Step 3** At the Phone Book (Speed Dial List) window, click an unassigned speed dial. The speed dial you selected is assigned to the contact number, and the speed dial code number appears next to the contact number.
 - Step 4** Click **Save**. To change a speed dial assignment, click the speed dial icon again and repeat Step 3.
-

Using System Settings

In addition to phone settings, the web page includes these areas for system management:

- Trace Logs—See [Viewing Trace Logs](#), page 4-34
- Backup Settings—See [Backup Settings for Phone Configuration](#), page 4-34
- Network Profiles—See [Using Network Profile Templates](#), page 4-35
- Phone Upgrade—See [Upgrading Phone Firmware](#), page 4-37
- Change Password—See [Changing the Admin Password](#), page 4-38
- Site Survey—See [Viewing the Site Survey Report on the Web](#), page 4-38
- Date and Time—See [Setting the Date and Time](#), page 4-19

For information about the remaining web page topics, see the [Chapter 9, “Monitoring the Cisco Unified Wireless IP Phone Remotely.”](#)

Viewing Trace Logs

You can use the Trace Logs area on the web page to view and manage trace files. System trace logs appear in a list on this page. You define how many messages are saved in the Trace Settings area.

To view a trace log, click on the “Message.<n>” link. The trace log appears in ASCII text. You can save the text file in a directory or on a disk to send to TAC for troubleshooting purposes.

To download a trace log, click **Download**. All the trace logs on the phone are then collected into a file named SEP<MAC-ADDRESS-OF-PHONE>_LOGS.tar.gz for a downloading and saving.



Note

Trace logs are erased when the phone is powered off. To preserve trace logs, see the [“Configuring Trace Settings”](#) section on page 4-27.

To display the Trace Logs area, access the web page for the phone as described in the [“Setting Up Your PC to Configure the Phones”](#) section on page 4-1, and then click the **Trace Logs** hyperlink.

Related Topics

- [Using System Settings](#), page 4-34
- [Backup Settings for Phone Configuration](#), page 4-34
- [Upgrading Phone Firmware](#), page 4-37
- [Changing the Admin Password](#), page 4-38

Backup Settings for Phone Configuration

You can use the Backup Settings area on the web page to export the phone configuration. You must set up an encryption key that encrypts the phone settings to keep them secure. When you export a configuration, all the settings in the network profiles, phone settings, USB settings, and trace are copied. None of the statistics or information fields are copied from the web pages.



Note

To import a file to a phone, you must enter the same encryption key that was used to export the file.

To display the Backup Settings area, access the web page for the phone as described in the “[Accessing the Configuration Web Page for a Phone](#)” section on page 4-5, and then click the **Backup Settings** hyperlink. Table 4-9 describes the items in this area.

Table 4-9 Backup Settings Area Items

Item	Description
Import Configuration	
Encryption Key	Enter the alphanumeric string up to 8-20 characters for encrypting the phone settings.
Import File	Enter the path and filename or use the Browse button to locate the file.
Import button	Click the button to import the phone settings file into the phone.
Export Configuration	
Encryption Key	Enter the alphanumeric string up to 8-20 characters for encrypting the phone settings.
Export button	Click the button to export the phone settings file to a location on your PC or to a disc.

Using Network Profile Templates

At initial phone deployment, you can create a typical network profile and export the phone settings to a location that you specify, such as a folder on your PC or your network. Then, you can import the network profile template to several phones to save time.

Creating a Configuration Template

To create a phone configuration template, follow these steps:

Procedure

- Step 1** Connect the USB cable to the phone and access the phone web page using the instructions on “[Accessing the Phone Web Page](#)” section on page 4-3.
- Step 2** On the phone web page, choose the **Network Profiles** hyperlink and configure the Network Profile settings for your template configuration.



Note You can leave the Username and Password fields blank so they can be configured individually.

- Step 3** Next, configure the USB Settings and Trace Settings for your template configuration.
- Step 4** Choose the **Backup Settings** hyperlink, to access the export and import settings.
- Step 5** In the Export Configuration area, enter an encryption key of from 8 to 20 characters. Record this key because you must enter this key to import the configuration template on other phones.
- Step 6** Click **Export** and the File Download dialog displays, and then click **Save**.
- Step 7** Give your configuration a new file name such as `7925template.cfg`.
- Step 8** Choose a location on your PC or on the network for the file and then click **Save**.

Step 9 The encrypted configuration file contains these settings:

- Profile Name
- SSID
- Single Access Point
- Call Power Save Mode
- 802.11 Mode
- WLAN Security
- Authentication Method
- User name
- Password
- Passphrase
- Encryption keys
- Use DHCP to get IP address and DNS servers
- Static Settings (if configured)
 - IP Address
 - Subnet Mask
 - Default Router
 - Primary DNS Server
 - Secondary DNS Server
- Use DHCP to get TFTP Server
- Static TFTP Settings (if configured)
 - TFTP Server 1
 - TFTP Server 2

Advanced Network Profile Settings

- Minimum PHY rate
- Surplus Bandwidth
- 802.11G Power Settings (checked ones)
- 802.11A Power Settings (checked ones)

USB Settings (use one of these)

- Obtain IP address from server
- or
- Static settings (if configured)
 - IP address
 - Subnet Mask

Trace Settings

- Number of Files
- Syslog Server (enabled/disabled)

- IP address
- Port
- Modules and error level for collection
- Preserving Logs (true/false)

Importing a Configuration Template

To import a phone configuration template, follow these steps:

Procedure

-
- Step 1** Connect the USB cable to an unconfigured phone and access the phone web page using the instructions on [“Accessing the Phone Web Page” section on page 4-3](#).
- Step 2** On the phone web page, choose the **Backup Settings** hyperlink.
- Step 3** In the Import Configuration area of the page, enter the Encryption Key.



Note You must enter the same key that you used to export the configuration template.

- Step 4** Use the Browse button to locate the configuration template and click **Open**.
The configuration file downloads to the phone.
- Step 5** You can use the web pages to add missing configuration items such as the username and password or make other changes at this time.
-

Related Topics

- [Using System Settings, page 4-34](#)
- [Viewing Trace Logs, page 4-34](#)
- [Upgrading Phone Firmware, page 4-37](#)
- [Changing the Admin Password, page 4-38](#)

Upgrading Phone Firmware

You can use the Phone Upgrade area on the web page to upgrade firmware files on the phones by using the USB connection or by using the WLAN.

To display the Phone Upgrade area, access the web page for the phone as described in the [“Accessing the Configuration Web Page for a Phone” section on page 4-5](#), and then click the **Phone Upgrade** hyperlink.

To upgrade the phone software, enter the phone software TAR (firmware file name) or use the Browse button to locate the firmware file on the network.

Related Topics

- [Using System Settings, page 4-34](#)
- [Viewing Trace Logs, page 4-34](#)

- [Backup Settings for Phone Configuration, page 4-34](#)
- [Changing the Admin Password, page 4-38](#)

Changing the Admin Password

Cisco Unified CallManager 4.x

If you are running Cisco Unified CallManager 4.x, you can use the Change Password area on the web page to change the administration password for the phone web pages.

To change the password on the web page, you must first enter the old password. Enter the new password and then reenter the new password to confirm the change.

To display the Change Password area, access the web page for the phone as described in the [“Accessing the Configuration Web Page for a Phone” section on page 4-5](#), and then click the **Change Password** hyperlink in the System sub-menu.

Cisco Unified Communications Manager 5.0, 5.1, 6.0, 6.1(1), or 7.0(1)

If you are running Cisco Unified Communications Manager 5.0, 5.1, 6.0, 6.1(1), or 7.0(1), you must set the password in Cisco Unified Communications Manager Administration on the Phone Configuration page. The password set in Cisco Unified Communications Manager takes precedence over the password that is set on the web pages.



Caution

When setting the Administration Password in the Product Specific Configuration section in Cisco Unified Communications Manager 5.0 Administration, you must enable TFTP encryption. Otherwise, the password appears in readable text in the phone configuration file and can be viewed from any host that has access to TFTP server.

Related Topics

- [Using System Settings, page 4-34](#)
- [Viewing Trace Logs, page 4-34](#)
- [Upgrading Phone Firmware, page 4-37](#)
- [Backup Settings for Phone Configuration, page 4-34](#)

Viewing the Site Survey Report on the Web

Before the Site Survey Report is generated for viewing from the phone web page, you must first run the Site Survey utility from the phone. For more information, see [Using the Site Survey Utility, page 2-24](#).

To view the report, go to the phone web page and choose **Site Survey** from the left pane. An HTML report in the form of a neighbor table of APs is displayed.



Note

You can also run the Neighbor List utility from the phone to display a list of current APs on the phone. However, this utility will not generate the Site Survey Report that you can access from the phone web page. See also [Using the Neighbor List Utility, page 2-23](#).

The neighbor table provides a matrix of APs observed during the site survey. Depending on the extent of the survey, not all observed APs will be considered a best AP or an immediate neighbor.

The Site Survey Report stores information about each AP until it reaches a limit of 256 APs. For each AP, up to ten neighbors are tracked.

Table 4-10 shows the information shown in the site survey report.

Table 4-10 Site Survey Report Neighbor Table

Information	Description/Indicator
Report title	The SSID used during Site Survey is displayed in the report title.
Best AP	Information displayed in cell with yellow background and where the row heading matches the column heading (for example, 64%-60/-43): <ul style="list-style-type: none"> Percentage of time it is the best AP. RSSI range during the time it is the best AP. <p>Note A low number (below -65) may indicate insufficient overlap between the best AP and its neighbors.</p>
Immediate Neighbor	Information may be displayed in the following way: <ul style="list-style-type: none"> Pink background— If AP is on the same channel as the best AP. <p>Note Being on the same channel as the best AP might indicate a problem with the channel re-use pattern, particularly if the percentage of time the AP is an immediate neighbor is relatively high compared to other immediate neighbors.</p> <ul style="list-style-type: none"> Asterisk (*)—Not an immediate neighbor. <p>Information displayed in cell (for example, 27%-61/-39):</p> <ul style="list-style-type: none"> Percentage of time it is the immediate neighbor of the best AP. RSSI range during the time it is the immediate neighbor.

Table 4-11 shows the information shown in the AP details report.

Table 4-11 AP Details Report

Field	Description
AP	Name of the AP if it is CCX-compliant; otherwise, the MAC address is displayed here.
MAC	MAC address of the AP.
Observation Count	Number of sweeps where this AP has been observed.
Channel - Frequency	The last channel and frequency where this AP was observed.
Country	A two-digit country code. Country information might not be displayed if the country information element (IE) is not present in the beacon.
Beacon Interval	Number of time units between beacons. A time unit is 1.024 ms.
DTIM Period	Every <i>n</i> th beacon is a DTIM period. After each DTIM beacon, the AP would send any broadcast or multicast packets that may have been queued for power-save devices.
RSSI Range [Lo Hi]	The entire RSSI range in which this AP has been observed.

Table 4-11 AP Details Report (continued)

Field	Description
BSS Lost Count	When a sweep does not discover an AP, the last best AP is flagged with a BSS lost count.
Channel Utilization	The percentage of time, normalized to 255, in which the AP sensed the medium was busy, as indicated by the physical or virtual carrier sense (CS) mechanism.
Station Count	Total number of spanning tree algorithms (STAs) currently associated with this BSS.
Available Admission Capacity	An unsigned integer that specifies the remaining amount of medium time available through explicit admission control, in units of 32 μ s/s.
Basic Rates	Data rates required by the AP at which the station must be capable of operating.
Optional Rates	Data rates supported by the AP that are optional for the station to operate at.
Multicast Cipher and Unicast Cipher	For Multicast Cipher, one of the following; for Unicast Cipher, one or more of the following: <ul style="list-style-type: none"> • None • WEP40 • WEP104 • TKIP • CCMP • CKIP CMIC • CKIP • CMIC
AKM	One or more of the following: <ul style="list-style-type: none"> • WPA1_1X • WPA_PSK • WPA2_1X • WPA2_PSK • WPA1_CCKM • WPA2_CCKM
Proxy ARP Supported	CCX compliant AP supports responding to IP ARP requests on behalf of the associated station. This feature is critical to standby time on the wireless IP phone.
WMM Supported	Support for WiFi Multi-Media Extensions.
CCX Version Number	Version of CCX if the AP is CCX compliant.

Table 4-11 AP Details Report (continued)

Field	Description
U-APSD Supported	Unscheduled Automatic Power Save Delivery is supported by the AP. May only be available if WMM is supported. This feature is critical to talk time and achieving maximum call density on the wireless IP phone.
Background AC	Access Category information for each AC: <ul style="list-style-type: none"> • Admission Control Required—If yes, admission control must be used prior to transmission using the access parameters specific for this AC. • AIFSN—Number of slots after an SIFS duration a non-AP STA should defer before invoking a backoff or starting a transmission. • ECWMIN—Encodes value of CWmin in an exponent form to provide the minimum amount of time in a random backoff. • ECWMAX—Encodes value of CWmax in an exponent form to provide the maximum amount of time in a random backoff. • TXOpLimit—Interval of time in which a particular quality of service (QoS) station has the right to initiate frame exchange sequences onto the wireless medium.
Best Effort AC	
Video AC	
Voice AC	
Channels	A list of supported channels (from the country IE).
Power	Maximum transmit power in dBm permitted for that channel.
Warning messages (in red at the bottom)	The first AP in the list (reference AP) is compared against the values recommended by Cisco, the differences are reported as warnings, and warning messages appear at the bottom of this report. All other APs are compared against the reference AP for consistency.



CHAPTER 5

Configuring Settings on the Cisco Unified Wireless IP Phone 7925G

This chapter describes the available configuration settings on the Cisco Unified Wireless IP Phone 7925G. It contains the following sections:

- [Accessing Network and Phone Settings, page 5-1](#)
- [Configuring Network Profile Settings, page 5-2](#)
- [Changing Phone Settings, page 5-10](#)
- [Configuring the Security Certificate on the Phone, page 5-12](#)
- [Changing the USB Configuration, page 5-13](#)

Accessing Network and Phone Settings

You can view and change many network configuration options and phone settings for the Cisco Unified Wireless IP Phone 7925G by using the Settings menu.





Note

You can control whether a Cisco Unified Wireless IP Phone 7925G has access to the Settings menu from the Cisco Unified Communications Manager Administration Phone Configuration page. Use the Settings Access field in the Product Specific Configuration section of the phone configuration page. For more information, see the [“Specific Configuration Options for the Cisco Unified Wireless IP Phone 7925G”](#) section on page 7-13.

To access the Settings menu, follow these steps:

Procedure

Step 1 Press  on the Navigation button for  (Settings).



Step 2 Use these menu options to view or change settings:

- **Phone Settings**
- **Network Profiles**
- **System Configuration**
- **Device Information**

- **Model Information**
- **Status**



Note These options are configurable; other options are display only.

- Step 3** To select the item that you want to configure or view, do one of these actions:
- Use the Navigation button to scroll to the item and then press the **Select** button.
 - Use the keypad to enter the number that corresponds to the item.
- Step 4** If a menu option is locked , you must press ** # on the keypad. When the menu is unlocked,  displays.

Related Topics

- [Configuring Network Profile Settings, page 5-2](#)
- [Changing Phone Settings, page 5-10](#)
- [Configuring the Security Certificate on the Phone, page 5-12](#)
- [Changing the USB Configuration, page 5-13](#)

Configuring Network Profile Settings

On the Cisco Unified Wireless IP Phone 7925G, you can configure four network profiles for a specific WLAN. Users who travel between company locations, can have separate network profiles for each WLAN location. You can set up profiles with the local SSID, WLAN settings, and authentication information for each location.



Note

You can control whether a Cisco Unified Wireless IP Phone 7925G has access to the Network Profiles menu from the Cisco Unified Communications Manager Administration Phone Configuration page. Use the Settings Access field in the Product Specific Configuration section of the phone configuration page. For more information, see the [“Specific Configuration Options for the Cisco Unified Wireless IP Phone 7925G”](#) section on page 7-13.




These sections provide information about configuring network profiles:

- [Accessing a Network Profile, page 5-3](#)
- [Changing the Profile Name, page 5-3](#)
- [Changing Network Configuration Settings, page 5-4](#)
- [Configuring DHCP Settings, page 5-6](#)
- [Configuring Wireless Settings for the Network Profile, page 5-8](#)

Accessing a Network Profile

To view or configure the Network Profile menu on a Cisco Unified Wireless IP Phone 7925G, follow these steps.

Procedure

-
- Step 1** Choose **SETTINGS > Network Profiles**.
- Step 2** To select the profile name that you want to configure, do one of these actions:
- Use the Navigation button to scroll to the item and then press the **Select** button.
 - Use the keypad to enter the number that corresponds to the item.
- The Network Config list is locked . To unlock the network settings in the profile, press * * # and  displays.
- Step 3** To display the profile settings, press **View**.
- Step 4** Scroll to and select one of these menu options:
- **Profile Name**
 - **Network Configuration**
 - **WLAN Configuration**
- Step 5** Make changes to the settings. For more information, see [Table 5-1](#).
- Step 6** To save changes to settings in the Profile menu, press **Save**.
- Step 7** To use the modified profile, scroll to the profile name and press **Select**. The  appears by enabled profiles. You can enable from 1 to 4 profiles.
-

Changing the Profile Name

You can change the default name of the network profile to one that is more meaningful to the user, such as, “Headquarters” or “Branch office.” You can change the name before or after you have made changes to the network profile.

To rename the profile, follow these steps.







Procedure

-
- Step 1** Choose **SETTINGS > Network Profiles**.
- Step 2** To select the profile name that you want to change, use the Navigation button to scroll to the item and then press the Select button.
- Step 3** Enter * * # to unlock the profile.
- Step 4** Select **Profile Name**.
- Step 5** Press the softkey to delete each character from right to left. Then enter the new profile name. See [Guidelines for Editing Settings in the Network Profile, page 5-4](#).

Step 6 Press **Options > Save** to complete the name change.

Guidelines for Editing Settings in the Network Profile

When you edit the Network Profile, you can enter characters, numbers, and special characters from the phone keypad. Use the numeric keys on the keypad to enter the number or the assigned characters. Each press moves to another character choice. Use the following guidelines when entering values:

- Enter characters—Press the numeric key to move to the desired character (lowercase, then upper case).
- Enter numbers—Press the numeric key to enter the number.
- Delete the last character—Press << to delete the last character or number in the string.
- Enter a space—Press  to enter a space between characters.
- Enter a dot—Press  to enter a dot between numbers.
- Enter special characters and symbols—Press one of the following keys to display and enter these characters:
 - Press  to enter * - / = \ ; ;
 - Press  to enter a space + , . ‘ “ | _ ~ ’
 - Press  to enter # ? () [] { }
 - Press  to enter ! @ < > \$ % ^ &
- Save an entry—Press **Options > Save**.
- Cancel editing mode—Press **Options > Cancel** as needed to return to the menu option or main screen.

Related Topics

- [Accessing Network and Phone Settings, page 5-1](#)
- [Configuring DHCP Settings, page 5-6](#)
- [Configuring an Alternate TFTP Server, page 5-7](#)
- [Configuring Wireless Settings for the Network Profile, page 5-8](#)

Changing Network Configuration Settings

After accessing a network profile, you can use [Table 5-1](#) for descriptions and reference information for network profile settings.

Table 5-1 Network Configuration Settings

Network Setting	Description	For More Information, See...
DHCP Server	IP address of the DHCP server from which the phone obtains its IP address	Configuring DHCP Settings, page 5-6
MAC Address	Unique MAC address of the phone	Display only, cannot configure

Table 5-1 Network Configuration Settings (continued)

Network Setting	Description	For More Information, See...
Host Name	Unique host name that the DHCP server assigned to the phone	Display only, cannot configure
DHCP Enabled	Yes—Allows the Dynamic Host Configuration Protocol (DHCP) to obtain an IP address for the phone No—Disables the use of DHCP. You must configure the static settings for the phone	Configuring DHCP Settings, page 5-6
IP Address	Internet Protocol (IP) address of the phone	Configuring DHCP Settings, page 5-6
Subnet Mask	Subnet mask used by the phone	
Default Router 1	Primary gateway used by the phone	
Domain Name	Name of the Domain Name System (DNS) domain in which the phone resides	
DNS Server 1	Primary DNS server used by the phone	
DNS Server 2	Optional backup DNS server used by the phone	Configuring an Alternate TFTP Server, page 5-7
Alternate TFTP	Yes—This option assigns an alternative Trivial File Transfer Protocol (TFTP) server No—This option uses the TFTP server assigned by DHCP	
TFTP Server 1	IP address for the primary TFTP server used by the phone. If you set Alternate TFTP option to Yes, you must enter a non-zero value for this option	
TFTP Server 2	Optional backup TFTP server the phone uses if the primary TFTP server is not available	
Load Server	IP address for the server where the phone receives firmware updates	<i>Cisco Unified Communications Manager Administration Guide.</i>
CDP Enabled	Enables or disables Cisco Discovery Protocol (CDP) for the phone in Cisco Unified Communications Manager Administration	Changing the Cisco Discovery Protocol Settings, page 5-7 <i>Cisco Unified Communications Manager Administration Guide.</i>
Erase Configuration	Deletes the phone configuration and sets to factory defaults	
Handset Only Mode	Yes—Indicates that the speakerphone is disabled on the phone No—Indicates that the speakerphone is enabled on the phone	Specific Configuration Options for the Cisco Unified Wireless IP Phone 7925G, page 7-13

Configuring DHCP Settings

The Cisco Unified IP Phones enable DHCP, by default, to automatically assign IP addresses to devices when you connect them to the network. If you do not use DHCP in your network, then you must disable DHCP and manually enter the network configuration information. For more information, see [“Interacting with the Dynamic Host Configuration Protocol Server” section on page 2-15](#).

Use these guidelines when manually configuring the IP settings:

- Ensure the TFTP server has an IP address.
- Ensure the default router IP address is on the same subnet as the host IP address.



Note

When DHCP is enabled, you cannot configure IP settings, but you can configure and alternate TFTP server.

Disabling DHCP

To disable DHCP on the phone and manually configure IP settings, follow these steps:

Procedure

- Step 1** Choose **SETTINGS >Network Profiles**.
- Step 2** Scroll to the profile name that you want to configure and press the **View** softkey.
- Step 3** Enter ****#** to unlock the profile and press the softkey to change.
- Step 4** Select **Network Configuration**. Press **View**.
- Step 5** Scroll to **DHCP Enabled** and press **No**.
- Step 6** Scroll to **IP Address** and press **Select**.
- Step 7** In the New IP Address: field, enter the static IP address for the phone.
- Step 8** Press **Options > Validate** to save the entry or press **Cancel**.

You must enter the other required static fields. See [Table 5-2](#) for descriptions of these fields.

For information about entering values, see the [“Guidelines for Editing Settings in the Network Profile” section on page 5-4](#).

Table 5-2 Static Settings When DHCP is Disabled

Static Setting	Description
IP Address	IP address, the unique identifier assigned by the system administrator for the phone.
Subnet Mask	Used to partition the IP address into a network identifier and host identifier so TCP/IP can distinguish between them.
Default Router 1	Identifies the gateway that provides connectivity to the IP network beyond the subnet to which the phone belongs.

Table 5-2 Static Settings When DHCP is Disabled (continued)

Static Setting	Description
Domain Name	Identifies the Domain Name System (DNS) domain in which the phone resides.
DNS Server 1 DNS Server 2	If the system is configured to use host names for servers instead of IP addresses, identify the primary and secondary DNS server to resolve host names.
Alternate TFTP server	Identifies whether you are using an alternate TFTP server. See Configuring an Alternate TFTP Server, page 5-7 .
TFTP Server 1	Identifies the TFTP server that the phone uses to obtain configuration files.

Configuring an Alternate TFTP Server

If you use DHCP to direct the Cisco Unified Wireless IP Phone 7925Gs to a TFTP server, you can also assign an alternative TFTP server to some phones instead of the one assigned by DHCP. To assign an alternate TFTP server to a phone, follow these steps:

Procedure

-
- Step 1** Choose **SETTINGS > Network Profiles**.
 - Step 2** To select the profile name that you want to configure, scroll to the item and then press the Select button.
 - Step 3** Enter ****#** to unlock the profile and press **Edit**.
 - Step 4** Select **Network Configuration**.
 - Step 5** Scroll to **Alternate TFTP** and press **Yes**.
 - Step 6** Scroll to **TFTP Server 1** and press **Select**.
 - Step 7** In the **New TFTP Server 1:** field, enter the IP address for the server.
See [Table 5-2](#) for descriptions of these fields.
For information about entering values, see the [“Guidelines for Editing Settings in the Network Profile” section on page 5-4](#).
 - Step 8** Press **Options > /Validate** to save the entry or press **Cancel**.
-

Changing the Cisco Discovery Protocol Settings

Some network devices do not use Cisco Discovery Protocol (CDP).

To change whether the phone transmits CDP packets and settings associated with CDP, follow these steps in Cisco Unified Communications Manager Administration:

Procedure

-
- Step 1** Choose **Device > Phone**.
 - Step 2** Click Find and locate the phone in the displayed list.

- Step 3** The Phone Configuration window displays for that phone.
 - Step 4** Scroll to Device Information.
 - Step 5** Scroll to Cisco Discovery Protocol Settings.
 - Step 6** Click Enabled from pull-down menu.
 - Step 7** Click Save and Reset if prompted.
-

Erasing the Configuration

You can erase the network profile configuration and return to the default settings.

To erase the configuration, follow these steps:

Procedure

-
- Step 1** Choose **SETTINGS > Network Profiles**.
 - Step 2** To select the profile name that you want to configure, scroll to the item and then press the Select button.
 - Step 3** Enter ****#** to unlock the profile and press **Edit**.
 - Step 4** Select **Network Configuration**.
 - Step 5** Scroll to **Erase Configuration** and press **Yes** to erase or **No**.
-

Related Topics

- [Changing the Profile Name, page 5-3](#)
- [Configuring Wireless Settings for the Network Profile, page 5-8](#)

Configuring Wireless Settings for the Network Profile

The WLAN Configuration menu contains settings that the phone uses to authenticate with an access point. These settings include the SSIDs, authentication type, and encryption data that the phone uses.

This section includes these topics for configuring wireless settings:

- [Accessing the WLAN Configuration Menu, page 5-8](#)
- [Changing WLAN Configuration Settings, page 5-9](#)

Accessing the WLAN Configuration Menu

To access the WLAN Configuration menu options on a Cisco Unified Wireless IP Phone 7925G, follow these steps:

Procedure

-
- Step 1** Choose **SETTINGS > Network Profiles**.
 - Step 2** To select the profile name that you want to configure, scroll to the item and then press the Select button.

- Step 3** Enter ****#** to unlock the profile and press **Edit**.
- Step 4** Scroll to and select **WLAN Configuration**.
- Step 5** To view or change the menu options, press **Edit**.
For descriptions of the settings, see [Table 5-3](#).
- Step 6** Press **Options > Save** to save the entry or press **Cancel**.

Changing WLAN Configuration Settings

After accessing the WLAN settings, use [Table 5-3](#) for descriptions and reference information for these settings.

Table 5-3 *WLAN Configuration Settings*

Network Setting	Description	For More Information, See...
SSID	Unique identifier for accessing wireless access points	Configuring Network Profiles, page 4-8
Security Mode	<p>The type of authentication that the phone uses to access the WLAN. Options are:</p> <ul style="list-style-type: none"> • Open—Access to all APs without WEP key authentication/encryption • Open+WEP—Access to all APs and authentication through WEP keys at the local AP • Shared Key+WEP—Shared key authentication through WEP keys at the local AP • LEAP—Exchanges a username and cryptographically secure password with a RADIUS server in the network (Cisco proprietary version of EAP) • EAP-FAST—Exchanges a username and cryptographically secure password with a RADIUS server in the network • EAP-TLS—Uses a dynamic session-based key derived from the client adapter and RADIUS server to encrypt data. Uses a client certificate for authentication. • PEAP—This method uses name and password authentication based on Microsoft MSCHAP V2 authentication. • Auto (AKM)—Phone selects the AP and type of key management scheme, either WPA, WPA2, WPA-PSK, WPA2-PSK, or CCKM that must use a wireless domain server (WDS) 	Configuring Wireless LAN Security, page 4-13
UserName	User name for the wireless network (up to 32 characters)	Configuring the Username and Password, page 4-15

Table 5-3 WLAN Configuration Settings (continued)

Network Setting	Description	For More Information, See...
Password	Password for the wireless network (up to 32 characters)	Configuring the Username and Password, page 4-15
802.11 Mode	The wireless signal standard used in the WLAN. Options are: <ul style="list-style-type: none"> • 802.11b/g • 802.11a • Auto-b/g • Auto-a • Auto-RSSI 	802.11 Standards for WLAN Communications, page 2-3
Call Power Save Mode	The type of power saving mode used in the WLAN. Options are: <ul style="list-style-type: none"> • U-APSD/PS-Poll • None 	Networking Protocols Used with Cisco Unified Wireless IP Phones, page 2-9
Scan Mode	Auto—Scans when on a call or when the strength signal (RSSI) is low. Continuous—Scans continuously even when it is not in a call. Single AP—Never scans except when the basic service set (BSS) is lost.	Wireless Network Requirements for VoIP, page 2-21

Related Topics

- [Accessing Network and Phone Settings, page 5-1](#)
- [Configuring Network Profile Settings, page 5-2](#)
- [Configuring the Security Certificate on the Phone, page 5-12](#)
- [Changing Phone Settings, page 5-10](#)

Changing Phone Settings

The Phone Settings menu enables configuration of individual phones with ring tones or volume levels, display settings, keypad settings, and home page settings.

**Note**

You can control whether a Cisco Unified Wireless IP Phone 7925G has access to the Phone Settings menu from the Cisco Unified Communications Manager Administration Phone Configuration page. Use the Settings Access field in the Product Specific Configuration section of the phone configuration page. For more information, see the [“Specific Configuration Options for the Cisco Unified Wireless IP Phone 7925G”](#) section on page 7-13.

To access the Phone Settings menu options on a Cisco Unified Wireless IP Phone 7925G, follow these steps:

Procedure

-
- Step 1** Choose **SETTINGS > Phone Settings**.
- Step 2** Press the number for the setting that you want to configure (or you can scroll to the setting and press the **Select** button).
- Step 3** Press the number for the setting category.
- Step 4** Press the number for the setting that you want to change.
-

For descriptions of the settings, see [Table 5-4](#). For specific instructions to change these settings, refer to “Using Phone Settings,” in the *Cisco Unified Wireless IP Phone 7925G Guide*.

Table 5-4 Configurable Settings for the Phone Sounds, Display, and Keypad

Phone Setting	Description
Sound Settings	
Ring Tone	Assigns the ring tone for each line on the phone.
Volumes	
Ring	Sets the ring volume level for the phone.
Speaker	Sets the volume for the speaker.
Handset	Sets the volume for the handset.
Headset	Sets the volume for the headset.
Alert Pattern	Sets the ring, vibrate, or combination to alert the user of an incoming call.
Ring Output	Sets the phone to ring through speaker, headset, or both speaker and headset.
Display Settings	
Display Brightness	Sets the brightness for the phone screen.
Display Timeout	Sets the length of time for the phone screen to display before turning off or disables the timer so screen always displays.
LED Coverage Indicator	Enables or disables the LED blink to indicate that the phone is in service and within the coverage area.
Keypad Settings	
Any Key Answer	Enables or disables using any key or button on the phone to answer a ringing call.
Keypad Auto Lock	Sets the length of time for the keypad to lock automatically after no keypad activity or disables auto lock.
Keypad Tone	Enables or disables tones for keypad presses.

Table 5-4 Configurable Settings for the Phone Sounds, Display, and Keypad (continued)

Phone Setting	Description
Customize Home Page	
Left Softkey	Enables Message or Phone Book on the home page.
Bluetooth	Enables or disables the Bluetooth functionality.

Related Topics

- [Accessing Network and Phone Settings, page 5-1](#)
- [Configuring Network Profile Settings, page 5-2](#)
- [Configuring the Security Certificate on the Phone, page 5-12](#)
- [Changing Phone Settings, page 5-10](#)

Configuring the Security Certificate on the Phone

Security 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.

A Locally Significant Certificate (LSC) installs on phones after you perform the necessary tasks that are associated with the Certificate Authority Proxy Function (CAPF). You can use Cisco Unified 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, ensure that the appropriate Cisco Unified Communications Manager and the 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.

Refer to *Cisco Unified Communications Manager Security Guide* for more information. For more information about the security features, see the [“Understanding Security Features for Cisco Unified IP Phones” section on page 1-8](#).

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

To configure an LSC on the phone, perform the following steps.

Procedure

-
- Step 1** Obtain the CAPF authentication string that was set when the CAPF was configured.
 - Step 2** Choose **SETTINGS > System Configuration > Security**.
 - Step 3** Press * * * # to unlock the option.
 - Step 4** Scroll to **LSC** and press the **Update** softkey.

The phone prompts for an authentication string.

Step 5 Enter the authentication string 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 appears 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, “Failed,” the authorization string may be incorrect or the phone may not be enabled for upgrading. Refer to error messages generated by the CAPF and take appropriate actions.

You can verify that an LSC is installed on the phone by choosing **SETTINGS > System Configuration > Security**. LSC displays Installed.

Related Topic

- [Understanding Security Features for Cisco Unified IP Phones, page 1-8](#)

Changing the USB Configuration

When using the USB cable to configure a phone, you might need to change the USB configuration. The phone has a default USB IP address of 192.168.1.100 that you can use with the USB connection to the PC. If you need to change the USB port configuration, these options are available:

- Obtain the IP address automatically, by getting an IP address from the PC with DHCP set up.
- Use the IP address and subnet mask assigned in this area.

To view or configure the USB port configuration on a Cisco Unified Wireless IP Phone 7925G, follow these steps:

Procedure

Step 1 Choose **SETTINGS > System Configuration > USB**.

Step 2 To open the menu, press the **Select** button.

Step 3 Press * * # to unlock the menu.

Step 4 To configure **DHCP**, press **Select** button and choose one of these options:

- To obtain an IP address automatically from the PC, choose **Enable**, then press **Save**. You have completed the USB configuration.
- To use a static IP address, choose **Disable**, then press **Save**.



Note If you disabled DHCP, you must enter an IP address and a subnet mask by performing Step 5 through 12.

Do not perform the following steps if DHCP is enabled.

- Step 5** To change the static IP address, scroll to **IP Address**, and press **Select** button.
- Step 6** Enter a new IP address that is not assigned on the subnet.
- Step 7** Press **Options > Validate** to verify the entry.
- Step 8** To save the changes, press **Save**.
- Step 9** To change the subnet for the new IP address, scroll to **Subnet Mask** and press **Select** button.
- Step 10** Enter the appropriate subnet address.
- Step 11** Press **Options > Validate** to verify the entry.
- Step 12** To save the changes, press **Save**.
-

Related Topics

- [Accessing Network and Phone Settings, page 5-1](#)
- [Configuring Network Profile Settings, page 5-2](#)
- [Configuring the Security Certificate on the Phone, page 5-12](#)
- [Changing Phone Settings, page 5-10](#)



CHAPTER 6

Configuring the Phone Using the Wavelink Avalanche Server

This chapter describes the Wavelink Avalanche Management Console and how to use it to configure the Cisco Unified Wireless IP Phone 7925G. The Cisco Unified Wireless IP Phone 7925G Configuration Utility (CU) can be installed on the Wavelink Avalanche Management Console and used to configure a single phone or multiple phones with common settings.

This chapter contains the following sections:

- [Before You Begin, page 6-1](#)
- [Best Practices, page 6-2](#)
- [Assigning the Wavelink Server, page 6-2](#)
- [Setting Up and Using the Phone CU, page 6-3](#)



Note

There is no support for Traffic Stream Rate Set (TSRS) or Cisco Compatible Extensions (CCX) V4.



Note

There are limitations using Wavelink because not all features are configurable. Some features are configurable only by using Cisco Unified Communications Manager Administration.

Before You Begin

Before you can use the Wavelink Avalanche Management Console to configure phones, ensure that you have the necessary components and follow the best practices during your setup.

The following components are required for configuring the phone using the Wavelink Avalanche server:

- Wavelink Avalanche software
 - Avalanche Manager Agent
 - Avalanche Management Console
- Cisco Unified Wireless IP Phone 7925G firmware release 1.1
- Cisco Unified Wireless IP Phone 7925G CU Avalanche Application Package
- DHCP server (optional)
- Cisco Unified Communications Manager (optional)

Best Practices

This section describes the best practices recommended for setting up and using the Cisco Unified Wireless IP Phone 7925G CU on the Wavelink Avalanche server.

- Ensure that the phone is registered to Cisco Unified Communications Manager.
- Try out this process with one or two phones before deploying to many phones.
- Set up a VLAN that only has access to the Wavelink server.
- Configure DHCP Option 149 with the Wavelink server IP address. If you do not configure this option, see [Assigning the Wavelink Server from the Phone, page 6-2](#).
- Configure a Cisco Access Point to use a default SSID of “cisco” with open authentication and no encryption.

Assigning the Wavelink Server

If you did not configure DHCP Option 149 with the Wavelink server IP address, you must manually assign it.



Note

Do not perform this task if you previously configured the Wavelink server address using DHCP Option 149.

To assign the Wavelink server on the phone, choose one of the following methods:

- [Assigning the Wavelink Server from the Phone, page 6-2](#)
- [Assigning the Wavelink Server using the Phone Web Page, page 6-3](#)

Assigning the Wavelink Server from the Phone

To assign the Wavelink server from the phone, follow these steps:

Procedure

-
- Step 1** Turn on the phone and verify that it is installed with the required firmware version and is registered to Cisco Unified Communications Manager.
 - Step 2** Choose **SETTINGS > System Configuration > Wavelink**.
 - Step 3** Unlock the phone by pressing ****#**.
 - Step 4** In the Alternate Wavelink Server option, choose **Yes**.
 - Step 5** Enter the IP address of the Wavelink server, and press **Save**.
-

Assigning the Wavelink Server using the Phone Web Page

To assign the Wavelink server using the phone web page, follow these steps:

Procedure

-
- Step 1** From the phone web page, choose **Wavelink Settings** from the left pane.
Under Wavelink Settings, make sure that the server is enabled.
- Step 2** Click **Use the following Server** and enter the IP address of the server, then click **Save**.
-

Setting Up and Using the Phone CU

This section describes the tasks for configuring and using the Cisco Unified Wireless IP Phone 7925G CU from the Wavelink Management Console.



Note

Be aware that the Cisco Unified Wireless IP Phone 7925G CU is labeled as 7921G but the CU works for both phones.

To set up and use the Cisco Unified Wireless IP Phone 7925G CU from the Wavelink Management Console, perform the tasks in [Table 6-1](#) in order.

Table 6-1 *Setting Up and Using the Phone CU on the Wavelink Console*

Task	For more information, see...
1. Assign attributes for the phone.	Assigning Attributes for the Phone, page 6-3
2. Install the Cisco Unified Wireless IP Phone 7925G CU on Wavelink.	Setting Up and Using the Phone CU, page 6-3
3. Update the configuration files.	Updating Configuration Files, page 6-5
4. Update the phones.	Assigning Attributes for the Phone, page 6-3

Assigning Attributes for the Phone

You can assign attributes on the Cisco Unified Wireless IP Phone 7925G that can be used to distinguish it from other mobile devices connected to the Wavelink server. These attributes can be used as search criteria for locating phones on the Wavelink server. For example, the predefined ModelName field of CP7925G is used to identify a device as the Cisco Unified Wireless IP Phone 7925G.

To assign attributes, use the Wavelink Management Console, the phone UI, or the phone web page:

- If you use the Wavelink Management Console, choose the Add Properties option from the Client Settings option (for a single phone) or the Edit Device Properties option (for a mobile device group). For more information, see the Wavelink Avalanche server documentation.
- If you assign attributes from the phone or phone web page, you define values for the CustomName and CustomValue fields:

- [Defining Custom Names and Custom Values on the Phone, page 6-4](#)
- [Defining Custom Parameters from the Phone Web Page, page 6-4](#)

Defining Custom Names and Custom Values on the Phone

To define the CustomName and CustomValue fields from the phone, follow these steps:

Procedure

-
- Step 1** On the main phone screen, choose **SETTINGS > System Configuration > Wavelink**.
- Step 2** Unlock the phone by pressing ****#**.
- Step 3** Scroll to a CustomName, enter an attribute name (for example, “User”), and click **Save**.



Note Only alphanumeric characters are allowed in the CustomName field.

- Step 4** Scroll to CustomValue and enter a value for the corresponding CustomName (for example, “Admin”), and click **Save**.

You can define up to four pairs of custom parameters.

Defining Custom Parameters from the Phone Web Page

To define customer parameters from the phone web page, follow these steps:

Procedure

-
- Step 1** From the phone web page, choose **Wavelink Settings**.
- Step 2** In the Wavelink Custom Parameters section, enter values in the Name and Value fields. You can define up to four pairs of custom parameters.



Note Do not use spaces in the Name field.

Installing the Cisco Unified Wireless IP Phone 7925G CU

The Cisco Unified Wireless IP Phone 7925G CU file is provided by Cisco in the .ava file format.



Note The phone CU must be installed on the Wavelink Avalanche Management Console.

To install the phone CU, follow these steps:

Procedure

-
- Step 1** Launch the Wavelink Avalanche Management Console and connect to the agent.
 - Step 2** Choose **Software Management > Install Software Package**.
 - Step 3** Browse to the location of the .ava file containing the Cisco Unified Wireless IP Phone CU and select it.
 - Step 4** Click **New** and enter the software collection name under which the phone configuration files will be added.
 - Step 5** Follow the instructions on the wizard to complete the installation.
 - Step 6** When the installation has completed, expand the software collection name on the left pane. The phone CU file name 7925CU appears with a red “x” (disabled) next to it.
 - Step 7** Right-click **7925CU** and choose **Enable Package**.



Note The installation is complete. As an option, you can perform the following additional steps to configure the selection criteria so you can easily apply changes to a device group.

-
- Step 8** Right-click the software collection (containing the phone CU) and choose **Settings**.
 - Step 9** Click the button at right of the Selection Criteria box to launch the Selection Criteria Wizard.
 - Step 10** Select an item from the Source Properties list on the left, and enter a value in the Selection Expression text box.
 - Step 11** Repeat the previous step for each property and value you wish to include. When finished, click **Compile**, then click **Test Expression**.
 - Step 12** Review the list displayed under Matching Clients to ensure the selection criteria have been met. Click **Apply**, then click **OK**.



Note For more information, see the Wavelink Avalanche Management Console documentation.

Updating Configuration Files

You can update a phone configuration file using the Cisco Unified Wireless IP Phone 7925G CU installed on a Wavelink Avalanche Management Console.

[Table 6-2](#) lists the configuration file settings.

Table 6-2 Configuration File Settings

Setting	For more information, see...
Profile Settings	Configuring Profile Settings, page 6-6
WLAN Settings	
Network Settings	

Table 6-2 Configuration File Settings

Setting	For more information, see...
USB Settings	Configuring USB Settings, page 6-9
Trace Settings	Configuring Trace Settings, page 6-9
Wavelink Settings	Configuring Wavelink Settings, page 6-10

To update settings in the phone configuration file, follow these steps:

Procedure

-
- Step 1** Right click **7925CU** (in a folder under Software Collections) to launch the CU.
 - Step 2** From the left pane, choose the settings you wish to configure: **Profile Settings**, **USB Settings**, **Trace Settings**, or **Wavelink Settings**.
 - Step 3** From the settings page, select or enter information for those settings.
 - Step 4** Click **Apply**.
-

Configuring Profile Settings

[Table 6-3](#) lists the profile settings.



Note

See also [Network Profile Settings, page 4-8](#), in the [Using the Cisco Unified Wireless IP Phone 7925G Web Pages](#) chapter.

Table 6-3 Profile Settings

Item	Description	For More Information, See...
Profile Name	Provides a name for the profile to make it easy to identify; up to 63 alphanumeric characters.	
Profile Enabled	Choose Yes or No .	
WLAN Settings		
SSID	Assigns the Service Set Identifier (SSID) to this profile. You must assign the same SSID to the phone that is also assigned to access points in the wireless network.	

Table 6-3 Profile Settings (continued)

Item	Description	For More Information, See...
WLAN Mode	<p>Determines the signal mode or priority for selecting signal modes available in the WLAN. Options are:</p> <ul style="list-style-type: none"> 802.11 b/g—Use only 2.4 GHz band 802.11a—Use only 5 GHz band Auto, 802.11b/g preferred over 802.11a (dual band) Auto, 802.11a preferred over 802.11b/g (dual band) <p>Note The preferred band, if available, will be used at power-on, but the phone may switch to the less preferred 2.4 GHz band, if available, and the preferred band is lost. Once the phone has connected to the less preferred band, it will not scan for the preferred band if the current band is acceptable, and may remain connected to the less preferred band.</p> <ul style="list-style-type: none"> Auto, signal strength (RSSI)—Use strongest signal in dual band environment 	802.11 Standards for WLAN Communications, page 2-3
Call Power Save Mode	<p>Set for the type of power saving mode used in the WLAN. Options are:</p> <ul style="list-style-type: none"> U-APSD/PS-Poll None 	802.11 Standards for WLAN Communications, page 2-3
WLAN Security		
Authentication Mode	<p>Sets the authentication and encryption methods for this profile:</p> <ul style="list-style-type: none"> Open—Open access to APs Open+WEP—Open access with WEP encryption (requires an encryption key) Shared+WEP—Shared key authentication with WEP (requires an encryption key) LEAP—Cisco proprietary authentication and encryption using a RADIUS server (requires a username and password) EAP-FAST—Authentication and encryption using TLS and RADIUS server (requires a username and password) Auto (AKM)—Automatic authenticated key management using: <ul style="list-style-type: none"> WPA, WPA2 (requires a username and password) WPA-Pre-shared key, WPA2-Pre-shared key (requires a passphrase/pre-shared key) CCKM (requires a username and password) 	
Wireless Security Credentials	Required for LEAP, EAP-FAST, and Auto (AKM) authentication methods	
Username	Assigns the network authentication username for this profile	

Table 6-3 Profile Settings (continued)

Item	Description	For More Information, See...
Password	Assigns the network authentication password for this profile	
WPA Pre-shared Key Credentials	Sets the Pre-shared key for this profile	
Pre-shared Key Type	Determines the key type: Hex or ASCII	
Pre-shared Key	Identifies the key	
Wireless Encryption	Required for Open+WEP and Shared+WEP authentication methods	
WEP Keys Type	Determines the encryption key type: Hex or ASCII	
WEP Keys TxKey	Identifies the Transmit Key.	
WEP Key Length 1-4	Determines the WEP key length with key size of 40 or 128 bits.	
WEP Key Value 1-4	Defines the WEP key value: <ul style="list-style-type: none"> • 40 bits—5 ASCII or 10 Hex characters • 128 bits—13 ASCII or 26 Hex characters 	
Network Settings		
DHCP Enabled	<ul style="list-style-type: none"> • Yes—Enables DHCP to obtain IP address and DNS servers automatically. • No—DHCP is disabled and you will need to enter the following fields: <ul style="list-style-type: none"> – IP Address – Subnet Mask – Default Router – Primary DNS – Secondary DNS – Domain Name 	
TFTP		
Alternate TFTP	<p>Determines whether DHCP assigns the TFTP server.</p> <p>If yes, enter static IP addresses for:</p> <ul style="list-style-type: none"> • TFTP Server 1 • TFTP Server 2 	
Advanced WLAN Settings		
TSPEC Settings		
Minimum PHY Rate	Minimum data rate that outbound traffic uses	
Surplus Bandwidth	Excess bandwidth beyond application requirements	
Antenna Settings		
Antenna Selection for 802.11A	<ul style="list-style-type: none"> • Vertical • Horizontal • Diversity 	

Table 6-3 Profile Settings (continued)

Item	Description	For More Information, See...
Antenna Selection for 802.11B	<ul style="list-style-type: none"> Vertical Horizontal Diversity 	
802.11G Power Settings	Enabled—Identifies enabled channels in WLAN to improve scanning for the phone Max Tx Power—Sets the maximum transmit power for the phone	
802.11A Power Settings	Enabled—Identifies enabled channels in WLAN to improve scanning for the phone Max Tx Power—Sets the maximum transmit power for the phone	

**Note**

If you uncheck all channels in the 802.11 G Power Settings or 802.11 A Power Settings, the phone will not be able to access the WLAN.

Configuring USB Settings

You can change the IP address of the USB port on your phone by choosing one of the following options in the DHCP Enabled field:

- Yes—Obtains an IP address automatically.
- No—You can specify the IP address and subnet mask on this page.

**Note**

See also [Configuring USB Settings, page 4-26](#).

Configuring Trace Settings

You can configure trace settings to determine how the phone creates and saves trace files. [Table 6-4](#) describes the trace settings.

Table 6-4 Trace Settings

Item	Description
Number of Files	Choose the number of trace files that the phone saves, from 2-10 files.
Enable Remote Syslog	Set up a remote server to store trace logs. If enabled, enter remote address and remote port.
Remote IP Address	Enter remote IP address if Enable Remote Syslog is enabled.
Remote Port	Enter a port number if Enable Remote Syslog is enabled. Valid values are: 514 and 1024 to 65535.

Table 6-4 Trace Settings (continued)

Item	Description
Kernel Level	Operating System data.
Configuration Level	Phone configuration data.
Call Control Level	Cisco Unified Communications Manager data.
Network Services Level	DHCP, TFTP, CDP data.
Security Level	Application level security data.
User Interface Level	Key strokes, softkeys, MMI data.
Wireless Level	Channel scanning, authentication data.
Audio Level	RTP, SRTP, RTCP, DSP data.
System Level	Firmware, upgrade data.

Configuring Wavelink Settings

You can configure Wavelink settings from the phone CU. [Table 6-5](#) describes the Wavelink settings.

Table 6-5 Wavelink Settings

Setting	Description
Enable	Enables the Wavelink server.
Use Alternate Server	Enables the use of alternate Wavelink server.
Alternate Server	If the User Alternate Server is enabled, enter an IP address for the alternate server.
Custom Name 1-4	Assign up to four attribute names to the phone to be used as selection criteria.
Custom Value 1-4	Define the values for each Custom Name to be used as selection criteria.

Updating the Phone

When you have completed the phone configuration changes, you must export the configuration file from the phone CU to Wavelink, and then update the phone.



Note

The Cisco Unified Wireless IP Phone 7925G CU does not perform a complete validation of the phone configuration. If the configuration file contains an invalid setting, the phone might reject the configuration and send an error message to the syslog.

To update the phone with the updated configuration file, perform the following steps.

Procedure

-
- Step 1** From the phone CU, select the configuration file, then choose **Export to Wavelink**.

- Step 2** At the Success window, click **OK**. A message indicating the file transfer is complete appears at the bottom of the window.
- Step 3** To update a mobile device group, select it from the left pane, and choose **Update Now (Disallow User Override)**.

To update a single device, expand a mobile device group or software collection from the left pane, right-click on the device listed in the right pane, and do one of the following:

- Choose **Update Now**.
 - Choose **Client Settings**. In the Avalanche Client Controls window, enable the Force package sync during Update Now checkbox, and click **Update Now**.
-



CHAPTER 7

Configuring Features, Templates, Services, and Users

This chapter provides an overview of the feature configuration and setup, softkey template modification, services set up, and user assignment in Cisco Unified Communications Manager Administration. Cisco Unified Communications Manager documentation provides detailed instructions for these procedures.

This chapter includes the following sections:

- [Configuring Cisco Unified Wireless IP Phones in Cisco Unified Communications Manager, page 7-1](#)
- [Telephony Features Available for the Phone, page 7-2](#)
- [Specific Configuration Options for the Cisco Unified Wireless IP Phone 7925G, page 7-13](#)
- [Configuring Softkey Templates, page 7-16](#)
- [Modifying Phone Button Templates, page 7-17](#)
- [Setting Up Services, page 7-17](#)
- [Configuring Corporate and Personal Directories, page 7-18](#)
- [Adding Users to Cisco Unified Communications Manager, page 7-19](#)
- [Managing the User Options Web Pages, page 7-20](#)
- [Creating Custom Phone Rings, page 7-21](#)

For suggestions about providing users with information for using the phone and features, see [Appendix A, “Providing Information to Users By Using a Website.”](#) For information about setting up phones in non-English environments, see [Appendix B, “Supporting International Users.”](#)

Configuring Cisco Unified Wireless IP Phones in Cisco Unified Communications Manager

To provide telephony call routing and call-control features for the Cisco Unified Wireless IP Phone 7925G, you must use Cisco Unified Communications Manager Administration. For instructions about adding these devices, refer to the “Cisco Unified IP Phone Configuration” chapter in the *Cisco Unified Communications Manager Administration Guide*.

Telephony Features Available for the Phone

Table 7-1 describes supported telephony features, that you can configure using Cisco Unified Communications Manager Administration for the Cisco Unified Wireless IP Phone 7925G. The table provides references to documentation that contains configuration procedures and feature information.

For information about using the features on the phone, refer to *Cisco Unified Wireless IP Phone 7925G Phone Guide and Quick Reference for Cisco Unified Communications Manager 4.3, 5.1, 6.0, 6.1, and 7.0(1)*. 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, you can use the **I or ? button** on the Cisco Unified Communications Manager configuration page.

Table 7-1 Telephony Features for the Cisco Unified Wireless IP Phone 7925G

Feature	Description	Configuration Reference
Abbreviated Dialing	Allows users to speed dial a phone number by entering an assigned code (1-99) on the phone keypad. Users assign the codes from the User Options web pages. See Speed dial, page 7-12 for more information.	For more information, refer to: <ul style="list-style-type: none"> • <i>Cisco Unified Communications Manager Administration Guide</i>, “Cisco Unified IP Phone Configuration” chapter. • <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phone” chapter.
Auto Answer	Connects incoming calls automatically after a ring or two to the speakerphone or headset if attached.	For more information, refer to the <i>Cisco Unified Communications Manager Administration Guide</i> : <ul style="list-style-type: none"> • For Cisco Unified Communications Manager 5.0 or later, refer to the “Configuring Directory Numbers” chapter. • For Cisco Unified Communications Manager 4.x, refer to the “Phone 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 Group Configuration” chapter.

Table 7-1 Telephony Features for the Cisco Unified Wireless IP Phone 7925G (continued)

Feature	Description	Configuration Reference
Barge	<p>Allows a user to join a non-private call on a shared phone line. Barge features include cBarge, Barge, and Single Button Barge.</p> <ul style="list-style-type: none"> cBarge adds a user to a call and converts it into a conference, allowing the user and other parties to access conference features. Barge adds a user to a call but does not convert the call into a conference. Single Button Barge enables users to Barge or cBarge into a remote-in-use call on a shared line. <p>The phones support Barge in two conference modes:</p> <ul style="list-style-type: none"> Built-in conference bridge at the target device (the phone that is being barged). This mode uses the Barge softkey. Shared conference bridge. This mode uses the cBarge softkey. <p>Note The Barge and Privacy features work together. See Privacy, page 7-11 for more information.</p>	<p>For more information, refer to:</p> <ul style="list-style-type: none"> <i>Cisco Unified Communications Manager Administration Guide</i>, “Device Pool Configuration” chapter. <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phones” chapter. <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Barge and Privacy” chapter.
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	<p>Allows a user to monitor the call state of a directory number (DN) associated with a speed-dial button. The available states are: alerting, idle, busy, and DND. During the alerting state, call pickup capability is enabled.</p> <p>Note This feature is not supported in Cisco Unified Communications Manager Release 4.x.</p>	For more information, refer to <i>Cisco Unified Communications Manager Features and Services Guide</i> , “Presence” chapter.
Call Back	Provides users with an audio and visual alert on the phone when a busy or unavailable party becomes available.	<p>For more information, refer to:</p> <ul style="list-style-type: none"> <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phones” chapter. <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Call Back” chapter.

Table 7-1 Telephony Features for the Cisco Unified Wireless IP Phone 7925G (continued)

Feature	Description	Configuration Reference
Call display restrictions	Determines the information that will display for calling or connected lines, depending on the parties who are involved in the call.	For more information, refer to: <ul style="list-style-type: none"> • <i>Cisco Unified Communications Manager Administration Guide</i>, “Cisco Unified IP Phone Configuration” chapter. • <i>Cisco Unified Communications Manager System Guide</i>, “Understanding Route Plans” chapter. • <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Call Display Restrictions” chapter.
Call forward	Allows users to redirect incoming calls to another number. Call forward options include Call Forward All, Call Forward Busy, Call Forward No Answer, and Call Forward No Coverage.	For more information, refer to: <ul style="list-style-type: none"> • <i>Cisco Unified Communications Manager Administration Guide</i>, “Directory Number Configuration” chapter. • <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phones” chapter. • Specifying Options that Appear on the User Options Web Pages, page 7-21
Call forward all loop breakout	Detects and prevents Call Forward All loops. When a Call Forward All loop is detected, the Call Forward All configuration is ignored and the call rings through.	For more information, refer to the <i>Cisco Unified Communications Manager System Guide</i> , “Cisco Unified IP Phones” chapter.
Call forward all loop prevention	Prevents a user from configuring a Call Forward All destination directly on the phone that creates a Call Forward All loop or that creates a Call Forward All chain with more hops than the existing <i>Forward Maximum Hop Count</i> service parameter allows.	For more information, refer to the <i>Cisco Unified Communications Manager System Guide</i> , “Cisco Unified IP Phones” chapter.
Call forward configurable display	Allows you to specify information that appears on a phone when a call is forwarded. This information can include the caller name, caller number, redirected number, and original dialed number.	For more information, refer to: <ul style="list-style-type: none"> • <i>Cisco Unified Communications Manager Administration Guide</i>. • <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phones” chapter.
Call forward destination override	Allows you to override Call Forward All in cases where the Call Forward All target places a call to the Call Forward All initiator. This feature allows the Call Forward All target to reach the Call Forward All initiator for important calls. The override works whether the Call Forward All target phone number is internal or external.	For more information, refer to “ <i>Cisco Unified Communications Manager System Guide</i> , “Cisco Unified IP Phones” chapter.

Table 7-1 Telephony Features for the Cisco Unified Wireless IP Phone 7925G (continued)


Feature	Description	Configuration Reference
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.	For more information, refer to: <ul style="list-style-type: none"> • <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phones” chapter. • <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Call Park” chapter.
Call pickup	Allows users to redirect a call that is ringing on another phone within their pickup group to their phone. You can configure an audio and/or visual alert for the primary line on the phone. This alert notifies the users that a call is ringing in their pickup group.  Note The audio/visual alert is only available for phones on Cisco Unified Communications Manager release 4.2 and later.	For more information, refer to: <ul style="list-style-type: none"> • <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Call Pickup Group Configuration” chapter. • <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phones” chapter. • <i>Cisco Unified Communications Manager Administration Guide</i>, “Cisco Unified IP Phone Configuration” 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.	For more information, refer to: <ul style="list-style-type: none"> • <i>Cisco Unified Communications Manager Administration Guide</i>, “Cisco Unified IP Phone Configuration” chapter (Release 4.x). • <i>Cisco Unified Communications Manager Administration Guide</i>, “Directory Number Configuration” chapter (Release 5.x and later). • <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phones” chapter.
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"> • <i>Cisco Unified Communications Manager Administration Guide</i>, “Configuring Cisco Unified IP Phones” chapter. • <i>Cisco Unified Communications Manager System Guide</i>, “Understanding Route Plans” chapter. • <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Call Display Restrictions” chapter.

Table 7-1 Telephony Features for the Cisco Unified Wireless IP Phone 7925G (continued)

Feature	Description	Configuration Reference
Calling Party Normalization	<p>Enables call backs to DNs that are routed through multiple geographical locations without having to modify the DN in the call log directories. DNs can be globalized and localized so that the appropriate calling number displays on the phone.</p> <p>To globalize a DN, use the international escape character, plus (+).</p>	<p>For more information, refer to:</p> <ul style="list-style-type: none"> • <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Calling Party Normalization” chapter. • <i>Cisco Unified Communications Manager System Guide</i>, “Using the International Escape Character +” chapter.
Client matter codes (CMC)	Enables a user to specify that a call relates to a specific client matter.	For more information, refer to the <i>Cisco Unified Communications Manager Features and Services Guide</i> , “Client Matter Codes and Forced Authorization Codes” chapter.
Conference	<p>Allows a user to talk simultaneously with multiple parties by calling each participant individually. Conference features include Conference, Join, cBarge, and Meet-Me.</p> <p>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.</p>	<ul style="list-style-type: none"> • For more information, refer to <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phones” chapter. • The Service parameter, AdvanceAdhocConference, (disabled by default in Cisco Unified Communications Manager Administration) allows you to enable these features. For more information, refer to the <i>Cisco Unified Communications Manager System Guide</i> “Conference Bridges” chapter. <p>Note 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.	<p>For more information, refer to:</p> <ul style="list-style-type: none"> • Cisco Unified Communications Manager 5.0 or later—<i>Cisco Unified Communications Manager Administration Guide</i>, “Directory Number Configuration” chapter • Cisco Unified Communications Manager 4.x—<i>Cisco Unified Communications Manager Administration Guide</i>, “Cisco Unified IP Phone Configuration” chapter. • <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phones” chapter.

Table 7-1 **Telephony Features for the Cisco Unified Wireless IP Phone 7925G (continued)**

Feature	Description	Configuration Reference
Direct transfer	Allows a user 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.
Directed Call Park	<p>Allows a user to transfer an active call to an available directed call park number that the user dials or speed dials. After pressing Transfer, the user dials the directed call park number to store the call.</p> <p>Call Park BLF speed dial enables access to the directed call park number and indicates that the directed call park number is available or unavailable.</p> <p>Note If you implement Directed Call Park, avoid configuring the Park softkey. This prevents users from confusing the two Call Park features.</p>	<p>For more information refer to:</p> <ul style="list-style-type: none"> • <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Call Park and Directed Call Park” chapter.
Do Not Disturb (DND)–Reject	Enables a user to temporarily busy out the phone when it is activated. If no call forwarding features are activated, calls to this station are routed to a busy signal or voice mail when DND–Reject is active. Otherwise, all incoming calls are routed to a preassigned call forwarding busy target.	<i>Cisco Unified CallManager Features and Services Guide</i> , “Do Not Disturb” chapter.

Table 7-1 Telephony Features for the Cisco Unified Wireless IP Phone 7925G (continued)

Feature	Description	Configuration Reference
DND	<p>When DND is turned on, 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.</p> <p>Note DND is available in Cisco Unified Communications Manager 6.0(1), 6.1(1), or 7.0(1) only.</p> <p>The following DND parameters are configurable in Cisco Unified Communications Manager Administration:</p> <ul style="list-style-type: none"> • DND—This checkbox allows you to enable DND on a per-phone basis. Use Cisco Unified Communications Manager Administration > Device > Phone > Phone Configuration. • DND Option—Choose “Call Reject” (to turn off all audible and visual notifications), or “Ringer Off” (to turn off only the ringer). DND Option appears on both the Common Phone Profile window and the Phone Configuration window (Phone Configuration window value takes precedence). • DND Incoming Call Alert—Choose the type of alert to play, if any, on a phone for incoming calls when DND is active. This parameter is located on both the Common Phone Profile window and the Phone Configuration window (Phone Configuration window value takes precedence). • BLF Status Depicts DND—Enables DND status to override busy/idle state. 	<p>For more information, refer to:</p> <ul style="list-style-type: none"> • <i>Cisco Unified CallManager Features and Services Guide</i>, “Do Not Disturb” chapter. • <i>Cisco Unified Communications Manager Administration Guide</i>.
Extension Mobility	<p>Enables users to sign into their DN from any Cisco Unified IP Phone. It also enables users to temporarily apply a phone number and user profile settings to a Cisco Wireless Unified IP Phone by logging into the Extension Mobility service on that phone.</p>	<p>For more information, refer to:</p> <ul style="list-style-type: none"> • <i>Cisco Unified Serviceability Administration Guide</i> • <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Cisco Unified Communications Manager Extension Mobility” chapter. • <i>Cisco Unified Communications Manager Business Edition</i>, “Cisco Extension Mobility” chapter.
Fast Dial Service	<p>Allows a user to enter a Fast Dial code to place a call. Fast Dial codes can be assigned to phone numbers or Personal Address Book entries. (See Services, page 7-12.)</p>	<p>For more information, refer to <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phone Services” chapter.</p>

Table 7-1 Telephony Features for the Cisco Unified Wireless IP Phone 7925G (continued)

Feature	Description	Configuration Reference
Forced authorization codes (FAC)	Controls the types of calls that certain users can place.	For more information, refer to <i>Cisco Unified Communications Manager Features and Services Guide</i> , “Client Matter Codes and Forced Authorization Codes” 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 Group Configuration” chapter.
Hold	Allows users to move connected calls from an active state to a held state.	Requires no configuration, unless you want to use music on hold; see Music on hold, page 7-11 .
Hold Reversion	<p>Limits the amount of time that a call can be on hold before reverting back to the phone that put the call on hold and alerting the user.</p> <p>Reverting calls are distinguished from incoming calls by a single ring (or beep, depending on the new call indicator setting for the line). This notification repeats at intervals if not resumed.</p> <p>A call that triggers Hold Reversion displays a brief message on the status line.</p> <p>You can configure call focus priority to favor incoming or reverting calls.</p>	For more information about configuring this feature, refer to <i>Cisco Unified CallManager Features and Services Guide</i> , “Hold Reversion” chapter.
Hunt group	Provides load sharing for calls to a main directory number. A hunt group contains a series of directory numbers that can answer the incoming calls. When the first directory number in the hunt group is busy, the system hunts in a predetermined sequence for the next available directory number in the group and directs the call to that phone.	<p>For more information, refer to:</p> <ul style="list-style-type: none"> • <i>Cisco Unified Communications Manager Administration Guide</i>, “Hunt Group Configuration” chapter. • <i>Cisco Unified Communications Manager System Guide</i>, “Understanding Route Plans” chapter.
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.	<p>For more information, refer to:</p> <ul style="list-style-type: none"> • <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phones” chapter. • <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Call Park and Directed Call Park” chapter

Table 7-1 Telephony Features for the Cisco Unified Wireless IP Phone 7925G (continued)

Feature	Description	Configuration Reference
Immediate Divert—Enhanced	Allows users to transfer incoming calls directly to their voice messaging system or to the voice messaging system of the original called party.	For more information, refer to: <ul style="list-style-type: none"> • <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phones” chapter. • <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Immediate Divert” chapter.
Intercom	Allows users to place and receive intercom calls from the line view. You can configure intercom lines to: <ul style="list-style-type: none"> • Directly dial a specific intercom extension. • Initiate an intercom call and then prompt the user to enter a valid intercom number. Users can view the intercom call history from the Directory menu.	For more information, refer to: <ul style="list-style-type: none"> • <i>Cisco Unified CallManager Feature and Services Guide</i>, “Intercom Configuration” chapter. • <i>Cisco Unified CallManager Feature and Services Guide</i>, “Cisco Extension Mobility” chapter.
Join Across Lines/Select	Allows users to apply the Join feature to calls that are on multiple phone lines.	For more information, refer to: <ul style="list-style-type: none"> • Refer to <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phones” chapter.
Join/Select	Allows user 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.
Log out of hunt groups	Allows users to log out of hunt groups and temporarily block calls from ringing their phone when they are not available to take calls. Logging out of hunt groups does not prevent non-hunt group calls from ringing their phones.	For more information, refer to <i>Cisco Unified Communications Manager System Guide</i> , “Understanding Route Plans” 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"> • <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phones” chapter. • <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Malicious Call Identification” chapter.
Meet-Me conference	Allows a user to host a Meet-Me conference in which other participants call a predetermined number at a scheduled time.	For more information refer to <i>Cisco Unified Communications Manager Administration Guide</i> , “Meet-Me Number/Pattern Configuration” chapter.

Table 7-1 **Telephony Features for the Cisco Unified Wireless IP Phone 7925G (continued)**

Feature	Description	Configuration Reference
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"> • <i>Cisco Unified Communications Manager Administration Guide</i>, “Message Waiting Configuration” chapter. • <i>Cisco Unified Communications Manager System Guide</i>, “Voice Mail Connectivity to Cisco Unified Communications Manager” chapter.
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. (See Call pickup, page 7-5 and Group call pickup, page 7-9.)	For more information refer to <i>Cisco Unified Communications Manager Features and Services Guide</i> , “Call Pickup Group Configuration” 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.
Privacy	Enables a user to allow or disallow other users of shared-line devices to view the device all information or to enable another user to barge into its active call.	For more information refer to: <ul style="list-style-type: none"> • <i>Cisco Unified Communications Manager Administration Guide</i>, “Cisco Unified IP Phone Configuration” chapter. • <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phones” chapter. • <i>Cisco Unified Communications Manager Features and Services Guide</i> “Barge and Privacy” chapter.
Push to Talk	Allows users to call a target phone number or group and announce a message (similar to a two-way radio) by using a configurable applications button.	For more information, see “Setting Up Services” section on page 7-17 . Requires an XML application to provide Push to Talk service.

Table 7-1 Telephony Features for the Cisco Unified Wireless IP Phone 7925G (continued)

Feature	Description	Configuration Reference
Quality Reporting Tool (QRT)	Allows users to use the QRT softkey on a phone to submit information about problem phone calls. QRT can be configured for either of two user modes, depending upon the amount of user interaction desired with QRT.	For more information refer to: <ul style="list-style-type: none"> • <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phones” chapter. • <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Quality Report Tool” chapter.
Redial	Allows users to call the most recently dialed phone number by using a softkey option.	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"> • <i>Cisco Unified Communications Manager 4.x Administration Guide</i>, “Cisco Unified IP Phone Configuration” chapter. • <i>Cisco Unified Communications Manager 5.x Administration Guide</i>, “Configuring Directory Numbers” chapter. • <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Custom Phone Rings” chapter. • “Creating Custom Phone Rings” section on page 7-21.
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"> • <i>Cisco Unified Communications Manager Administration Guide</i>, “Cisco Unified IP Phone Configuration” chapter. • <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phone Services” chapter.
Shared Line	Allows users to have multiple phones that share the same phone number or allows users 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 dial	Dials a specified number that has been previously stored. Speed dialing includes these features: <ul style="list-style-type: none"> • Speed-dial hot keys configured and stored in the local Phone Book on the wireless IP phone. • Line view speed-dial numbers configured from the User Options web page. See Abbreviated Dialing, page 7-2 and Fast Dial Service .	For more information refer to: <ul style="list-style-type: none"> • <i>Cisco Unified Communications Manager Administration Guide</i>, “Cisco Unified IP Phone Configuration” chapter. • <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phones” chapter.

Table 7-1 **Telephony Features for the Cisco Unified Wireless IP Phone 7925G (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"> • <i>Cisco Unified Communications Manager Administration Guide</i>, “Time Period Configuration” chapter. • <i>Cisco Unified Communications Manager System Guide</i>, “Time-of-Day Routing” chapter.
Transfer	Allows users to redirect connected calls from their phones to another number.	Requires no configuration.
Voice message system	Enables callers to leave messages if calls are unanswered.	For more information refer to: <ul style="list-style-type: none"> • <i>Cisco Unified Communications Manager Administration Guide</i>, “Cisco Voice-Mail Port Configuration” chapter. • <i>Cisco Unified Communications Manager System Guide</i>, “Voice Mail Connectivity to Cisco Unified Communications Manager” chapter.

Related Topics

- [Configuring Softkey Templates, page 7-16](#)
- [Setting Up Services, page 7-17](#)
- [Configuring Corporate and Personal Directories, page 7-18](#)
- [Adding Users to Cisco Unified Communications Manager, page 7-19](#)
- [Creating Custom Phone Rings, page 7-21](#)

Specific Configuration Options for the Cisco Unified Wireless IP Phone 7925G

Each Cisco Unified IP Phone has special configuration options in Cisco Unified Communications Manager Administration that are available by phone model. The following product specific configuration options are available for the Cisco Unified Wireless IP Phone 7925G:

- **Disable Speakerphone**—Turns off the speakerphone capability of the handset. Options are False or True.
- **Gratuitous ARP**—Enables or disables the ability for the phone to learn MAC addresses from Gratuitous ARP. This capability is required to monitor or record voice streams. Options are Enabled or Disabled.

- **Settings Access**—Enables, disables, or restricts access to local configuration settings in the Settings menus. With restricted access, only the Phone Settings menu is accessible. With disabled access, no options appear when you access the Settings menu on the phone. Options are Enabled, Disabled, and Restricted.
- **Web Access**—Determines the level of access to the web pages for the phone. Provides Disabled, Read only, and Full access to a phone's web pages through a web browser. Options are Read Only, Full, Disabled.
- **Profile 1-4**—Locks or unlocks the network profiles. If locked, the phone user cannot modify the network profile. Options are Unlocked and Locked.
- **Load Server**—Identifies the alternate server that the phone will use to obtain firmware loads and upgrades. Enter an IP address or host name for the server.
- **Admin Password (Cisco Unified Communications Manager 5.0 and later)**—Password to access the configuration web pages for the phone. Default password is "CiscoCisco." Password must be 8-32 characters.

**Caution**

When setting the Administration Password in the Product Specific Configuration section in Cisco Unified Communications Manager Administration 5.0 or later, you must enable TFTP encryption. Otherwise, the password appears in readable text in the phone configuration file and can be viewed from any host that has access to TFTP server.

- **Special Numbers**—Identifies special phone numbers that do not require unlocking the keypad to call, such as 911 or an emergency number. Enter numbers up to 16 digits in length.
- **Application URL**—Specifies the URL that the phone contacts application services. The maximum length is 256 characters.
- **"Send" Key Action**—Enables onhook dialing which displays a list of the last numbers dialed on the phone; offhook dialing which sends an SCCP offhook message to the Cisco Unified Communications Manager server.
- **Days Display Not Active**—Specifies the days that the backlight is off by default. The list contains all the days of the week. To turn off the backlight on the specified days, use the Control key plus the days.
- **Display On Time**—Indicates the time of day the display turns on automatically.
- **Display On Duration**—Indicates the amount of time the display is active. No value indicates the end of a day. Maximum value is 24 hours. Input the number of hours and minutes, for example 1:30 would indicate a display time of 1 hour and 30 minutes.
- **Display Idle Timeout**—Specifies when the display times out after a configurable amount of inactivity. It continually resets if the phone is active. The default is to time out after 1 hour. Maximum value is 24 hours. Input the number of hours and minutes, for example 1:30 would indicate a display time of 1 hour and 30 minutes.
- **Phone Book Web Access**—Controls the access of the local phone book so that it can be accessed by using the web page for the phone. It works with the Web Access parameter. When Web Access is disabled, the local phone book is not accessible.
- **Unlock-Settings Sequence (**#)**—Specifies the unlock settings as **#. The phone cannot be unlocked using any other sequence if this parameter is enabled. The user does not have write-access to the phone Settings menu if this parameter is enabled unless the sequence is entered on the phone.
- **Application Button Activation Timer**—Specifies the amount of time to hold down the Application Button to active the application. The values are seconds.

- **Application Button Priority**—Indicates the priority of the Application Button relative to the other phone tasks. The Low option specifies that the Application Button works only when the phone is idle and on the main screen. The Medium option specifies that the button takes precedence over all tasks except when the keypad is locked. The High option specifies that the button takes precedence over all tasks on the phone.
- **Out-of-Range Alert**—Controls the frequency of audible alerts when the phone is out of range of an AP. The phone does not play audible alerts when the parameter value is “disabled.” The phone can beep once or regularly at 10, 30, or 60 second intervals. Once the phone is within range of an AP, the alert stops.
- **Scan Mode**—Controls the scanning by the phone. The parameter values are as follows: Auto: Phone scans when it is in a call or when the received strength signal indicator (RSSI) is low. Single AP: Phone never scans except when the basic service set (BSS) is lost. Continuous: Phone scans continuously even when it is not in a call. The default is Auto.
- **Restricted Data Rate**—Enables or disables the restriction of the upstream and downstream PHY rates according to CCX V4 Traffic Stream Rate Set IE (S54.2.6). The default is disabled.
- **Power Off When Charging**—Indicates whether the phone powers off when it is connected to a charger or placed in a charging station. The default is disabled.
- **Cisco Discovery Protocol**—Enables or disables the Cisco Discovery Protocol on the phone. The default is enabled.
- **Advertise G.722 Codec**—Indicates whether the phone advertises the G.722 codec to the Cisco Unified Communications Manager. Codec negotiation involves two steps: first, the phone must advertise the supported codec to the Cisco Unified Communications Manager (not all endpoints support the same set of codecs). Second, when the Cisco Unified Communications Manager gets the list of supported codecs from all phones involved in the call attempt, it chooses a commonly supported codec based on various factors, including the region pair setting. Valid values are: Use System Default (defers to the setting specified in the enterprise parameter, Advertise G.722 Codec), Disabled (does not advertise G.722 to the Cisco Unified Communications Manager) or Enabled (advertises G.722 to the Cisco Unified Communications Manager). The default is Use System Default.
- **Home Screen**—Enables two views on the phone: Main Phone Screen or Line View. The default is the Main PHone Screen.

To configure product specific options, follow these steps:

Procedure

-
- Step 1** Do one of the following from Cisco Unified Communications Manager Administration:
- For Cisco Unified Communications Manager 4.x or earlier, choose **Device > Phone**. Click **Add a Phone**, then choose **Phone Type > Cisco7925**.
 - For Cisco Unified Communications Manager 5.0 and later, choose **Device > Phone**. Click **Add Phone**, then choose **Phone Type > Cisco7925**.
- Step 2** In the Phone Configuration page, locate the **Product Specific Configuration** area.
- Step 3** Make changes to the settings as needed.



Note For detailed information about these settings, click the **I or ? button** for Product Specific Configuration Help.

Step 4 You must reset the phone before the changes take effect.

Configuring Softkey Templates

Administrators can change the order of softkeys for the Cisco Unified Wireless IP Phone 7925G by using Cisco Unified Communications Manager Administration. Unlike other Cisco Unified IP Phones that have buttons for some functions, the Cisco Unified Wireless IP Phone 7925G has two non-configurable softkeys that are set for:

- Message
- Options

When you configure a softkey template for the Cisco Unified Wireless IP Phone 7925G, you can only configure the Cisco Unified Communications Manager softkeys and their sequence in the Options menu. The order of softkeys in the softkey template corresponds to the phone softkey list in the Options menu. When you set up the softkey template for users that prefer to have a particular softkey appear during a connected call, place the desired softkey in the first position for the Connected phone state.

Softkey Templates for the Cisco Unified Wireless IP Phone 7925G

The standard softkey template displays the Hold softkey when connected to a call. Some users want the Transfer softkey to appear for a connected call instead of Hold.

The administrator sets up a non-standard softkey template that places Transfer in the first position for the Connected state. The administrator assigns this non-standard softkey template to the Cisco Unified Wireless IP Phone 7925G assigned to users that want these softkeys.



Note

To ensure that users hear the voice-messaging greeting when they are transferred to the voice message system, you must set up a softkey template with Transfer as the first softkey for a connected call.

Changing Softkeys in a Template

Use the procedures in the online Help topic, “Adding Non-Standard Softkey Templates” to change the softkeys and their sequence. Softkey templates now support up to 16 softkeys when using applications. For more information about softkey templates, see the “Softkey Templates” Chapter in the *Cisco Unified Communications Manager System Guide*.

To configure softkey templates, select **Device > Device Settings > Softkey Template** from Cisco Unified Communications Manager Administration. 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 assign a softkey template to a phone, use the Softkey Template field in the Cisco Unified Communications Manager Administration Phone Configuration page. Refer to the “Softkey Template Configuration” chapter in the *Cisco Unified Communications Manager Administration Guide* and the *Cisco Unified Communications Manager System Guide* for more information.

Related Topics

- [Specific Configuration Options for the Cisco Unified Wireless IP Phone 7925G, page 7-13](#)
- [Setting Up Services, page 7-17](#)
- [Configuring Corporate and Personal Directories, page 7-18](#)
- [Adding Users to Cisco Unified Communications Manager, page 7-19](#)

Modifying Phone Button Templates

Phone button templates let you assign lines and features to positions in the Line View. Ideally, you modify templates before registering phones on the network. In this way, you can access customized phone button template options from Cisco Unified Communications Manager during registration.

To modify a phone button template, choose **Device > Device Settings > Phone Button Template** from Cisco Unified Communications Manager Administration. To assign a phone button template to a phone, use the Phone Button Template field in the Cisco Unified Communications Manager Administration Phone Configuration page. For more information about modifying phone button templates, refer to “Cisco Unified IP Phones” chapter in the *Cisco Unified Communications Manager System Guide* for your release.

The Cisco Unified Wireless IP Phone 7925G can have up to six lines and up to 24 connected calls. The default button template uses position 1 for lines and assigns position 2 through 6 as speed dial. You can assign these features to button positions:

- Service URL
- Privacy
- Speed dial

Use softkey features in the Options menu to access other phone features, such as call park, call forward, redial, hold, resume, conferencing, and so on.

Setting Up Services

The Services menu on the Cisco Unified Wireless IP Phone 7925G 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 Push to Talk, directories, stock quotes, and weather reports. Some services, such as Push to Talk, can use the configurable Applications button located on the side of the phone.

To create customized XML applications for your site, refer to the [Cisco Unified IP Phone Service Application Development Notes](#).

Before a user can access any service, two important tasks must be completed:

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

To set up IP Phone services, follow these steps:

Procedure

-
- Step 1** 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.
- Step 2** To set up these services in Cisco Unified Communications Manager 4.x Administration, choose **Feature > Cisco IP Phone Services**
or
To set up these services in Cisco Unified Communications Manager 5.x Administration, choose **Device > Device Settings > Phone Services**
- For more information about phone services, refer to the “Cisco Unified IP Phone Services” chapter in the *Cisco Unified Communications Manager System Guide* for more information.
- Step 3** After you configure these services, verify that your users have access to the Cisco Unified Communications Manager User Options web-based application, from which they can select and subscribe to configured services. See the “[How Users Configure Phone Features and Services](#)” section on page A-4 for a summary of the information that you must provide to end users.
-



Note

For information about extension mobility services for users, refer to the “Cisco Extension Mobility” chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

Related Topics

- [Specific Configuration Options for the Cisco Unified Wireless IP Phone 7925G](#), page 7-13
- [Configuring Softkey Templates](#), page 7-16
- [Configuring Corporate and Personal Directories](#), page 7-18
- [Adding Users to Cisco Unified Communications Manager](#), page 7-19
- [Creating Custom Phone Rings](#), page 7-21

Configuring Corporate and Personal Directories

The **Directory** menu on the Cisco Unified Wireless IP Phone 7925G 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 7-19 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 7-19 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. That manual guides you through the configuration process for integrating Cisco Unified Communications Manager with Microsoft Active Directory, Sun ONE Directory, Netscape Directory, and iPlanet Directory Server.

After the LDAP directory configuration completes, users can use the Corporate Directory service on your Cisco Unified Wireless IP Phone 7925G 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 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 Configure Phone Features and Services](#)” section on page A-4 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 > Installation** 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 TabSynInstall.exe file to all users who require this application.

Adding Users to Cisco Unified Communications Manager

Adding users to Cisco Unified Communications Manager Administration allows you to display and maintain information about users and allows each user to perform the following actions:

- Access the corporate directory and other customized directories from a Cisco Unified IP Phone
- Create a personal directory
- Set up speed dial and call forwarding numbers
- Subscribe to services that are accessible from a Cisco Unified IP Phone

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

- To add users individually from Cisco Unified Communications Manager Administration for 5.0 or later, choose **User Management > End User > Add New**.

To add users individually from Cisco Unified Communications Manager Administration for 4.x, choose **User > Add a New User**.

Refer to “Adding a New User” chapter in *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.

For detailed information, refer to *Bulk Administration Tool User Guide* (Cisco Unified Communications Manager 4.1 or later) or *Cisco Unified Communications Manager Bulk Administration Guide* (Cisco Unified Communications Manager 5.0 or later).

Related Topics

- [Specific Configuration Options for the Cisco Unified Wireless IP Phone 7925G, page 7-13](#)
- [Configuring Softkey Templates, page 7-16](#)
- [Configuring Corporate and Personal Directories, page 7-18](#)
- [Adding Users to Cisco Unified Communications Manager, page 7-19](#)
- [Creating Custom Phone Rings, page 7-21](#)

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 Wireless IP Phone 7925G 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. To do so, choose **User Management > User Group**. You must also associate appropriate phones with the user.

To perform this procedure, do the following:

Cisco Unified Communications Manager Administration for Release 5.x and Later

-
- Step 1** Choose **User Management > End User**.
 - Step 2** Add the username.
 - Step 3** Add the phone.
 - Step 4** Associate the phone to the user.
 - Step 5** Add the user to a user group.
-

For Cisco Unified Communications Manager Administration for Release 4.x, refer to *Cisco Unified Communications Manager Administration Guide*, “End User Configuration” section.

**Note**

You can use Cisco Unified Communications Manager Administration to control user access to the phone web pages. For information about setting Web Access for users, see [“Specific Configuration Options for the Cisco Unified Wireless IP Phone 7925G”](#) section on page 7-13.

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).
- **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.

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 the “Custom Phone Rings” chapter in the *Cisco Unified Communications Manager Features and Services Guide* for more information about customized ring tones.

Related Topics

- [Specific Configuration Options for the Cisco Unified Wireless IP Phone 7925G, page 7-13](#)

- [Configuring Softkey Templates, page 7-16](#)
- [Configuring Corporate and Personal Directories, page 7-18](#)
- [Adding Users to Cisco Unified Communications Manager, page 7-19](#)
- [Creating Custom Phone Rings, page 7-21](#)



CHAPTER 8

Viewing Security, Device, Model, Status, and Call Statistics Information on the Phone

This chapter describes how to use the Settings menus on the Cisco Unified Wireless IP Phone 7925G to view the Security Configuration menu, Device Information menu, Model Information menu, Status menu, and the Call Statistics screen. This chapter includes the following sections:

- [Viewing Security Information, page 8-1](#)
- [Viewing Device Information, page 8-4](#)
- [Viewing Model Information, page 8-7](#)
- [Viewing the Phone Status Menu, page 8-8](#)

For more information, see [Chapter 9, “Monitoring the Cisco Unified Wireless IP Phone Remotely.”](#) For more information about troubleshooting the Cisco Unified IP Phone, [Chapter 10, “Troubleshooting the Cisco Unified Wireless IP Phone 7925G.”](#)

Viewing Security Information

To view the Security Configuration screen on the Cisco Unified Wireless IP Phone 7925G and see information about the security settings, follow these steps:

Procedure

- Step 1** Choose the **SETTINGS > System Configuration > Security**.
 - Step 2** Use the Navigation button to scroll through the items in the Security Configuration screen.
 - Step 3** [Table 8-1](#) describes the items that appear in this screen.
 - Step 4** To exit the Security Configuration screen, press the **Back** softkey.
-





Table 8-1 Security Configuration Screen Items

Item	Description
Web Access	<p>Indicates web access capability for the phone.</p> <ul style="list-style-type: none"> • Disabled—No user options web page access • ReadOnly—Can view information • Full—Can use configuration pages <p>You configure web access in Cisco Unified Communications Manager Administration.</p>
Security Mode	<p>Displays the security mode that is set for the phone. You configure the device security mode in Cisco Unified Communications Manager Administration.</p> <p>Note If you choose PEAP as your security mode, you can enable the validation of the server certificate on the phone.</p>
MIC	<p>Indicates whether a manufacturing installed certificate (used for the security features) is installed on the phone (Yes) or is not installed on the phone (No). For information about how to manage the MIC for your phone, refer to the “Using the Certificate Authority Proxy Function” chapter in <i>Cisco Unified Communications Manager Security Guide</i>.</p>
LSC	<p>Indicates whether a locally significant certificate (used for the security features) is installed on the phone or is not installed on the phone. For information about how to manage the LSC for your phone, refer to the “Using the Certificate Authority Proxy Function” chapter in <i>Cisco Unified Communications Manager Security Guide</i>.</p>
CTL File	<p>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 Not Installed. (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 the “Configuring the Cisco CTL Client” chapter in <i>Cisco Unified Communications Manager Security Guide</i>.)</p> <p>If a CTL file is installed on the phone, also provides access to the CTL File screen. For more information, see the “Accessing the CTL File Screen” section on page 8-3.</p>
Trust List	<p>If a CTL file is installed on the phone, provides access to the Trust List screen. For more information, see the “Trust List Screen” section on page 8-4.</p>
CAPF Server	<p>Displays the IP address or host name and the port of the CAPF that the phone uses.</p>

Accessing the CTL File Screen

If a CTL file is installed on the phone, you can access the CTL File screen by choosing **Settings > System Configuration > Security > CTL File**. To exit the CTL File screen, press the **Exit** softkey.

The CTL File screen contains these options:

- **CTL File**—Displays the MD5 hash of the certificate trust list (CTL) file that is installed in the phone, and provides access to the CTL File menu. If no CTL file is installed on the phone, this field displays Not Installed. (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*.)
 - 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.
- **CAPF Server**—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/TFTP Server**—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.

If neither the primary TFTP (TFTP Server 1) server nor the backup TFTP server (TFTP Server 2) is 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 or to the TFTP Server 2 option on the Network Configuration menu. (For information about changing these options, see the [“Configuring DHCP Settings” section on page 5-6.](#))



Note

When the wireless IP phone is connected to a Cisco Unified Communications Manager Release 5.0 or later, you can have multiple security profiles assigned to a phone. When the phone has more than one security profile using different secure Cisco Unified Communications Manager clusters, you must delete the CTL file from the current profile before enabling another profile. See [“Understanding Security Profiles” section on page 1-12.](#)

To unlock the CTL file from the Security Configuration screen, follow these steps:

Procedure

-
- Step 1** Scroll to the CTL File menu and press **Select**.
 - Step 2** Press ****#** to unlock options on the CTL File menu.
If you decide not to continue, press ****#** again to lock options on this menu.
 - Step 3** Scroll to the CTL option that you want to change and press **Erase**.
After you make the change, the CTL file will be locked automatically.
-




Trust List Screen

The Trust List screen 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 screen by choosing **Settings > Security Configuration > Trust List**.

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

The Trust List screen contains these options:

- CAPF Server—IP address of the CAPF used by the phone. Also displays a certificate  icon if a certificate is installed for this server.
- Communications Manager / TFTP Server—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.
- SRST Router—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 server.

Related Topics

- [Viewing the Status Messages, page 8-9](#)
- [Viewing Call Statistics, page 8-14](#)
- [Viewing Firmware Versions, page 8-16](#)

Viewing Device Information

You can access the Device Information screen on the Cisco Unified Wireless IP Phone 7925G and to view information about the current configuration:

- Cisco Unified Communications Manager servers
- Network settings
- WLAN information
- HTTP information
- Locale information
- Security settings
- QoS information

To view the Device Information screen, follow these steps:

Procedure

-
- Step 1** Choose **Settings menu > Device Information**.
- Step 2** Use the Navigation button to scroll to one of the categories in the Device Information screen and press **Select**.
- The list of items under the category displays.
- Step 3** [Table 8-2](#) describes the categories and items that appear in this screen.

Step 4 To exit the Device Information screen, press the **Back** softkey.

Table 8-2 *Device Information Categories and Items*

Item	Description
CallManager Information	
CallManager 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.</p> <p>Each available server displays the Cisco Unified Communications Manager server IP address and one of the following states:</p> <ul style="list-style-type: none"> • Active—Cisco Unified Communications Manager server from which the phone is currently receiving call-processing services. • Standby—Cisco Unified Communications Manager server to which the phone switches if the current server becomes unavailable. • Blank—No current connection to this Cisco Unified Communications Manager server.
Network Information	
DHCP Server	IP address of the DHCP server from which the phone obtains its IP address.
MAC Address	MAC address of the phone.
Host Name	Unique, fixed name that is automatically assigned to the phone based on the MAC address.
Domain Name	Name of the DNS in which the phone resides.
IP Address	IP address of the phone.
Subnet Mask	Subnet mask used by the phone.
TFTP Server 1	Primary TFTP server used by the phone.
TFTP Server 2	Secondary TFTP server used by the phone.
Default Router 1	IP address for the default gateway used by the phone.
DNS Server 1	Primary DNS server used by the phone.
DNS Server 2	Backup DNS server used by the phone.
Load Server	Host name or IP address for the alternate server that the phone uses for firmware upgrades.
CDP Enabled	Indicates whether the network is using Cisco Discovery Protocol (CDP).
DHCP Enabled	Indicates whether this phone is using DHCP for its IP address assignment or not.
Alternate TFTP	Indicates whether this phone uses a TFTP server other than the one assigned by DHCP.

Table 8-2 Device Information Categories and Items (continued)

Item	Description
WLAN Information	
Profile Name	Name of the network profile that the phone is currently using.
SSID	Service Set ID that the phone is currently using.
802.11 Mode	Wireless signal mode that the phone is currently using.
Single Access Point	Indicates if the phone minimizes scanning (Enabled) or scans for APs frequently (Disabled).
Call Power Save Mode	Type of power save mode that the phone uses to save battery power—PS-Poll or U-APSD.
Security Mode	Authentication method that the phone is currently using in the wireless network.
Encryption Type	Encryption method that the phone is currently using in the wireless network.
Key Management	Encryption key management that the phone is currently using in the wireless network.
Tx Power	Transmit power setting for the phone.
HTTP Information	
Directories URL	URL of the server from which the phone obtains directory information.
Services URL	URL of the server from which the phone obtains Cisco Unified IP Phone services.
Messages URL	URL of the server from which the phone obtains message services.
Information URL	URL of the help text that appears on the phone.
Authentication URL	URL that the phone uses to validate requests made to the phone web server.
Proxy Server URL	Not used.
Idle URL	Not used.
Locale Information	
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.
User Locale Version	Version of the user locale loaded on the phone.
Network Locale Version	Version of the network locale loaded on the phone.
Security Information	
GARP Enabled	Indicates whether the phone learns MAC addresses from Gratuitous ARP responses.
Security Mode	Security mode assigned to the phone.

Table 8-2 *Device Information Categories and Items (continued)*

Item	Description
Web Access	Indicates web access capability for the phone. <ul style="list-style-type: none"> • Disabled—No user options web page access • ReadOnly—Can view information only • Full—Can use configuration pages You configure web access in Cisco Unified Communications Manager Administration.
QoS Information	
DSCP for Call Control	Differentiated Services Code Point (DSCP) IP classification for call control signaling.
DSCP for Configuration	DSCP IP classification for any phone configuration transfer.
DSCP for Services	DSCP IP classification for phone-based service.

Related Topics

- [Viewing Security Information, page 8-1](#)
- [Viewing Model Information, page 8-7](#)
- [Viewing the Phone Status Menu, page 8-8](#)

Viewing Model Information

You can view the Model Information screen on the Cisco Unified Wireless IP Phone 7925G to see information about the hardware and software.

To view this screen, follow these steps:

Procedure

-
- Step 1** Choose **SETTINGS > Model Information**.
- Step 2** Use the Navigation button to scroll through the items in the Model Information screen.
- Step 3** [Table 8-3](#) describes the items that appear in this screen.
- Step 4** To exit the Model Information screen, press the **Back** softkey.
-

Table 8-3 *Model Information Screen Items*

Item	Description
Model Number	Model number of the phone.
MAC Address	MAC address of the phone.
App Load ID	Identifier of the factory-installed load running on the phone.
Serial Number	Serial number of the phone.

Table 8-3 Model Information Screen Items (continued)

Item	Description
WLAN Regulatory Domain	Identifier for the wireless regulatory domain in which this phone must operate. <ul style="list-style-type: none"> • 1050—North America • 3051—Europe (ETSI) • 4157—Japan • 5252—World mode including Australia/New Zealand, Asia, and Pacific
USB Vendor ID	Unique code that identifies the vendor as a Cisco Systems.
USB Product ID	Unique code that identifies the phone as a Cisco Systems product.
RNDIS Device Address	Manufacturer-assigned unique MAC address for the USB Remote Network Driver Interface Specification (RNDIS) for the phone.
RNDIS Host Address	Manufacturer-assigned unique MAC address for the USB RNDIS for the host.

Related Topics

- [Viewing Security Information, page 8-1](#)
- [Viewing Device Information, page 8-4](#)
- [Viewing the Phone Status Menu, page 8-8](#)

Viewing the Phone Status Menu

The Status menu includes the following 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 [“Viewing the Status Messages” section on page 8-9](#).
- **Network Statistics**—Displays the Network Statistics screen, which shows Ethernet traffic statistics. For more information, see the [Viewing Network Statistics, page 8-12](#).
- **Call Statistics**—Displays the Call Statistics screen, which shows counters, statistics, and voice quality metrics. For more information, see the [Viewing Call Statistics, page 8-14](#).
- **Firmware Versions**—Displays the Firmware Versions screen, which shows information about the firmware running on the phone. For more information, see the [Viewing Firmware Versions, page 8-16](#).
- **Neighbor List**—Displays the the neighboring APs and information on currently connected APs. See [Using the Neighbor List Utility, page 2-23](#).
- **Site Survey**—Displays the wireless media across all channels and locates APs that belong to the Basic Service Set (BSS). See [Using the Site Survey Utility, page 2-24](#).
- **Trace Settings**—Displays the debug information for the phone. The following must be enabled in:
 - Remote syslog
 - Trace levels

- Preserve logs
- Preserve trace levels

Viewing the Status Messages

You can use the Settings menu and Status menu to view status messages for the Cisco Unified Wireless IP Phone 7925G. The Status Messages screen displays up to 10 of the most recent status messages that the phone has generated.

You can access this screen at any time, even if the phone has not finished starting up. [Table 8-5](#) describes the status messages that might appear. This table also includes actions you can take to address indicated errors.

To view status messages, follow these steps:

-
- Step 1** Choose **Settings > Status**.
- Step 2** Select **Status Messages**; the list of the status messages displays.
To erase the messages, press the **Clear** softkey
- Step 3** To exit the screen, press the **Back** softkey.
-

Table 8-4 Status Message, Description, and Possible Explanation and Action

Status Message	Description	Possible Explanation and Action
Bad MIC on phone	The manufacturing installed certificate (MIC) that is used for security features is bad.	For information about how to manage the MIC for your phone, refer to the “Using the Certificate Authority Proxy Function” chapter in <i>Cisco Unified Communications Manager Security Guide</i> .
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"> • Phone is not registered with Cisco Unified Communications Manager. You must manually add the phone to Cisco Unified Communications Manager if you are not allowing phones to auto-register. See the “Methods for Adding Phones to Cisco Unified Communications Manager” section on page 3-2 for details. • If you are using DHCP, verify that the DHCP server is pointing to the correct TFTP server. • If you are using static IP addresses, check configuration of the TFTP server. See the “Configuring IP Network Settings” section on page 4-23 for details on assigning a TFTP server.
CTL Installed	A certificate trust list (CTL) file is installed in the phone.	<p>None. This message is informational only.</p> <p>For more information about the CTL file, refer to <i>Cisco Unified Communications Manager Security Guide</i>.</p>
CTL update failed	The phone could not update its certificate trust list (CTL) file.	<p>Problem with the CTL file on the TFTP server.</p> <p>For more information, refer to <i>Cisco Unified Communications Manager Security Guide</i>.</p>
Duplicate IP	Another device is using the IP address assigned to the phone.	<ul style="list-style-type: none"> • If the phone has a static IP address, verify that you have not assigned a duplicate IP address. See the “Configuring IP Network Settings” section on page 4-23 section for details. • If you are using DHCP, check the DHCP server configuration.

Table 8-4 Status Message, Description, and Possible Explanation and Action

Status Message	Description	Possible Explanation and Action
LCS operation failed	The locally significant certificate (LSC) that is used for the security features did not install properly.	For information about how to manage the LSC for your phone, refer to the “Using the Certificate Authority Proxy Function” chapter in <i>Cisco Unified Communications Manager Security Guide</i> .
LCS operation complete	The LCS was updated successfully on the phone.	For information about how to manage the LSC for your phone, refer to the “Using the Certificate Authority Proxy Function” chapter in <i>Cisco Unified Communications Manager Security Guide</i> .
TFTP Error	The phone does not recognize an error code provided by the TFTP server.	Contact the Cisco TAC.
TFTP server not authorized	The specified TFTP server could not be found in the phone CTL.	<ul style="list-style-type: none"> • The DHCP server is not configured properly and is not providing the correct TFTP server address. In this case, update the TFTP server configuration to specify the correct TFTP server. • 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. • 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.
TFTP timeout	TFTP server did not respond.	<ul style="list-style-type: none"> • Network is busy—The errors should resolve themselves when the network load reduces. • No network connectivity between the TFTP server and the phone—Verify the network connections. • TFTP server is down—Check configuration of TFTP server.

Viewing the Current Configuration

You can use the Settings menu and Status menu to determine the name of the configuration file for the Cisco Unified Wireless IP Phone 7925G.

To locate the configuration file name, follow these steps:

Procedure

Step 1 Choose **SETTINGS > Status**.

Step 2 Select **Status Messages**.

The phone displays the name of the configuration file in the following format:

SEPmacaddress.cnf.xml or SEPmacaddress.cnf.xml.enc.sgn.

Step 3 To exit the screen, press the **Back** softkey.

Related Topics

- [Viewing the Status Messages, page 8-9](#)
- [Viewing Network Statistics, page 8-12](#)
- [Viewing Call Statistics, page 8-14](#)
- [Viewing Firmware Versions, page 8-16](#)

Viewing Network Statistics

You can use the Settings menu and Status menu to view information about the phone and network performance.

To view the Network Statistics follow these steps:

Procedure

Step 1 Press the **SETTINGS > Status**.

Step 2 Select **Network Statistics**; the list of statistics displays.

Step 3 Use the Navigation button to scroll through the items in the Network Statistics screen.

Step 4 [Table 8-5](#) describes the items that appear in this screen.

Step 5 To exit the Network Statistics screen, press the **Back** softkey.

Table 8-5 Network Statistics Screen Items

Item	Description
Up Time	Amount of elapsed time in days and hours since the phone connected to Cisco Unified Communications Manager
RxPkts	Number of packets received by the phone

Table 8-5 Network Statistics Screen Items (continued)

Item	Description
RxErr	Number of errored packets received by the phone
RxUcast	Number of unicast packets received by the phone
RxMcast	Number of multicast packets received by the phone
RxBcast	Number of broadcast packets received by the phone
FcsErr	Number of packets with frame checksum (FCS) errors
Tx Failed	Number of packet transmissions that failed
RcvBeacons	Number of beacons received by the phone
AssocRej	Number of AP association rejections
AssocTmOut	Number of AP association timeouts
AuthRej	Number of authentication rejections
AuthTmOut	Number of authentication timeouts
The following network statistics items display these AP queues: Best Effort (BE), Background (BK), Video (VI), and Voice (VO).	
TxPkts	Number of packets transmitted by the phone
TxErr	Number of transmit errors
TxUcast	Number of unicast packets transmitted by the phone
TxMcast	Number of multicast packets transmitted by the phone
TxBcast	Number of broadcast packets transmitted by the phone
RTSFail	Number of request to send (RTS) failures
ACKFail	Number of packet acknowledgements that failed
Retry	Number of times the phone retried to send packets
MRetry	Number of times the phone retried to send multicast packets
RetryFail	Number of times the phone retried and failed to send packets
AgedPkts	Number of packets removed from the transmit queue due to transmission timeout
OtherFail	Number of packets that failed to transmit due to other reasons
Success	Number of packets successfully transmitted
MaxFail	Maximum sequence of failure due to maximum retry limit

Related Topics

- [Viewing the Status Messages, page 8-9](#)
- [Viewing Call Statistics, page 8-14](#)
- [Viewing Firmware Versions, page 8-16](#)

Viewing Call Statistics

You can access the Call Statistics screen on the phone to display counters, statistics, and voice quality metrics in these ways:

- During call—You can view the call information by pressing the Select 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 9, “Monitoring the Cisco Unified Wireless 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 **SETTINGS > Status**.
- Step 2** Scroll to and select **Call Statistics**; the list of statistics appears.
- Step 3** Use the Navigation button to scroll through the items in the Call Statistics screen. [Table 8-6](#) describes the items that appear in this screen.
- Step 4** To exit the Call Statistics screen, press the **Back** softkey.

Table 8-6 Call Statistics Items

Item	Description
RxType	Type of voice stream received (RTP streaming audio): G.729, G.722/iLBC, G.711 u-law, G.711 A-law, or Lin16k.
TxType	Type of voice stream transmitted (RTP streaming audio): G.729, G.722/iLBC, G.711 u-law, G.711 A-law, or Lin16k.
Rcvr Size	Size of voice packets, in milliseconds, in the receiving voice stream (RTP streaming audio).
Sender Size	Size of voice packets, in milliseconds, in the transmitting voice stream.
Rcvr Packets	Number of RTP voice packets received since voice stream was opened. Note 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.

Table 8-6 Call Statistics Items (continued)

Item	Description
Sender Packets	Number of RTP voice packets transmitted since voice stream was opened. Note 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.
Avg Jitter (value1/value2)	Estimated average RTP packet jitter (dynamic delay that a packet encounters when going through the network). <ul style="list-style-type: none"> Value 1 is the average jitter in milliseconds (ms). Value 2 is the current audio frame buffer depth in millisecond (ms).
Max Jitter	Maximum jitter observed since the receiving voice stream was opened.
Rcvr Discarded	Number of RTP packets in the receiving voice stream that have been discarded (bad packets, too late, and so on). Note The phone will discard payload type 19 comfort noise packets that are generated by Cisco Gateways, which will increment this counter.
Rcvr Lost Packets	Missing RTP packets (lost in transit).
Voice Quality Metrics	
MOS LQK	Score that is an objective estimate of the mean opinion score (MOS) for listening quality (LQK) that rates from 5 (excellent) to 1 (bad). This score is based on audible concealment events due to frame loss in the preceding 8-second interval of the voice stream. For more information, see the “Monitoring the Voice Quality of Calls” section on page 10-12. Note The MOS LQK score can vary based on the type of codec that the Cisco Unified IP Phone uses.
Avg MOS LQK	Average MOS LQK score observed for the entire voice stream.
Min MOS LQK	Lowest MOS LQK score observed from start of the voice stream.
Max MOS LQK	Baseline or highest MOS LQK score observed from start of the voice stream. These codecs provide the following maximum MOS LQK score under normal conditions with no frame loss: <ul style="list-style-type: none"> G.711 gives 4.5 G.729 A /AB gives 3.7
MOS LQK Version	Version of the Cisco proprietary algorithm used to calculate MOS LQK scores.
CumConcealRatio	Total number of concealment frames divided by total number of speech frames received from start of the voice stream.

Table 8-6 Call Statistics Items (continued)

Item	Description
IntConcealRatio	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.
MaxConcealRatio	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).
SevConcealSecs	Number of seconds that have more than 5 percent concealment events (lost frames) from the start of the voice stream.

Related Topics

- [Viewing the Status Messages, page 8-9](#)
- [Viewing Network Statistics, page 8-12](#)
- [Viewing Firmware Versions, page 8-16](#)

Viewing Firmware Versions

You can verify the firmware versions that are used on the Cisco Unified Wireless IP Phone 7925G by viewing the Firmware Info screen. The firmware version name is in this format:

`Product_Name-Model-Protocol.Version Number.Filetype`

An example of the firmware release for the Cisco Unified Wireless IP Phone 7925G is `cmterm-7925-sccp.X-0-0.cop.sgn`.

[Table 8-7](#) explains the information that is displayed on this screen.

To display the firmware information, follow these steps:

Procedure

-
- Step 1** Choose **SETTINGS > Status**.
- Step 2** Select **Firmware Versions**.
- To view one of the items, scroll to the item and press **Select**.
- Step 3** To exit the Firmware Versions screen, press **Back**.
-

Table 8-7 Firmware Version Information

Item	Description
App Load ID	Identifies the phone firmware version running in the phone
Boot Load ID	Identifies the factory-installed load running on the phone
WLAN Driver ID	Identifies the version of the wireless LAN driver
WLAN Firmware ID	Identifies the Wireless LAN firmware version running in the phone

Related Topics

- [Viewing the Status Messages, page 8-9](#)
- [Viewing Network Statistics, page 8-12](#)
- [Viewing Call Statistics, page 8-14](#)



CHAPTER 9

Monitoring the Cisco Unified Wireless IP Phone Remotely

This chapter describes the methods for monitoring the Cisco Unified Wireless IP Phone 7925G by using a web page. It contains the following sections:

- [Accessing the Web Page for a Phone, page 9-1](#)
- [Summary Information, page 9-2](#)
- [Network Configuration Information, page 9-3](#)
- [Device Information, page 9-6](#)
- [Wireless LAN Statistics, page 9-7](#)
- [Wireless LAN Statistics, page 9-7](#)
- [Stream Statistics, page 9-10](#)

For information about using these web pages, see [Chapter 4, “Using the Cisco Unified Wireless IP Phone 7925G Web Pages.”](#) For more information about troubleshooting the Cisco Unified IP Phone, [Chapter 10, “Troubleshooting the Cisco Unified Wireless IP Phone 7925G.”](#)

Accessing the Web Page for a Phone

To access the web page for a Cisco Unified Wireless IP Phone 7925G, perform the following steps.

Procedure

- Step 1** Obtain the IP address of the Cisco Unified Wireless IP Phone 7925G using one of these methods:
- Search for the phone in Cisco Unified Communications Manager by choosing **Devices > Phones**. 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 Wireless IP Phone 7925G, press **SETTINGS > Device Information > Network** 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:
- `https://<IP_address>`



Note When the Security Alert dialog box displays a notice to accept the Trust Certificate, click **Yes** or **Always** to accept the application.

Step 3 Log in to the web pages with username: **admin** and enter the password: **Cisco** for the phone web pages.

The web pages for a Cisco Unified Wireless IP Phone 7925G includes these items for monitoring the phone:

- Wireless LAN Statistics—Provides information about the wireless LAN configuration. For more information, see the [“Wireless LAN Statistics” section on page 9-7](#).
- Network Statistics—Provides information about network traffic. For more information, see the [“Wireless LAN Statistics” section on page 9-7](#).
- Stream Statistics—Provides information about voice quality items. For more information, see the [“Stream Statistics” section on page 9-10](#).

Summary Information

The Summary Information area on the phone’s web page displays network configuration information and information about other phone settings. [Table 9-1](#) describes these items.

To display the Summary Information page, access the web page for the phone as described in the [“Accessing the Web Page for a Phone” section on page 9-1](#), and the Home: Summary page displays.

Table 9-1 Home: Summary Items

Item	Description
Phone DN	Directory number assigned to this phone
Wireless Information	
Active Network Profile	Name of the profile that the phone is currently using
SSID	SSID that the phone is currently using
Access Point	Name of the access point to which the phone is associated
MAC Address	Media Access Control (MAC) address of the phone
Network Information	
IP Address	Internet Protocol (IP) address of the phone
Subnet Mask	Subnet mask used by the phone
Default Router	IP address for the default gateway that the phone is using
TFTP Server	IP address for the Primary Trivial File Transfer Protocol (TFTP) server that the phone is using
Communications Manager Information	
Active Communications Manager	IP address for the Cisco Unified Communications Manager server to which the phone is registered
Phone Directory Number	Primary directory number for the phone

Network Configuration Information

The Network Setup area on the phone's web page displays network configuration information and information about other phone settings. [Table 9-2](#) describes these items.

To display the Network Information page, access the web page for the phone as described in the [“Accessing the Web Page for a Phone”](#) section on page 9-1, and then click the **Network** hyperlink under the Information section.

Table 9-2 Network Information Items

Item	Description
IP Information	
DHCP Server	IP address of the Dynamic Host Configuration Protocol (DHCP) server from which the phone obtains its IP address.
BootP Server	Not used.
MAC Address	Media Access Control (MAC) address of the phone.
Host Name	Unique, fixed name that is automatically assigned to the phone based on the MAC address.
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.
Default Router 1	IP address for the default gateway used by the phone.
DNS Server 1	Primary Domain Name System (DNS) server used by the phone.
DNS Server 2	Backup DNS server used by the phone.
TFTP Server 1	Primary Trivial File Transfer Protocol (TFTP) server used by the phone.
Alternate TFTP Server Enabled	Displays Yes if enabled and No if disabled.
TFTP Server 2	Secondary Trivial File Transfer Protocol (TFTP) server used by the phone.

Table 9-2 Network Information Items (continued)

Item	Description
Communications Manager Information	
CallManager 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>Each available server shows the Cisco Unified Communications Manager server IP address and one of the following states:</p> <ul style="list-style-type: none"> • Active—Cisco Unified Communications Manager server from which the phone is currently receiving call-processing services. • Standby—Cisco Unified Communications Manager server to which the phone switches if the current server becomes unavailable. • Blank—No current connection to this Cisco Unified Communications Manager server.

Table 9-2 Network Information Items (continued)

Item	Description
SRST Information	
SRST Reference IP	The IP Address for 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. 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.
SRST Reference Port	Port number for TCP connection.
SRST Reference Option	Identifies the default gateway or disables SRST.
Connection Monitor Duration	The amount of time that the IP phone monitors its connection to Cisco Unified Communications Manager before it unregisters from SRST and re-registers to Cisco Unified Communications Manager.
MLPP Information	
MLPP Domain ID	Identifies the MLPP Domain that is assigned to the phone.
MLPP Indication Status	Indicates whether the phone uses special precedence rings and tones.
Preemption	Identifies call preemption capability set for this phone. Forceful—The phone allows higher priority calls to preempt lower priority calls. Disabled—The phone does not preempt lower priority calls with higher priority calls. Default—The phone uses the device pool setting.
QoS Information	
DSCP for Call Control	Differentiated Services Code Point (DSCP) IP classification for call control signaling.
DSCP for Configuration	DSCP IP classification for any phone configuration transfer.
DSCP for Services	DSCP IP classification for phone-based service.
Security Information	
GARP Enabled	Indicates whether the phone learns MAC addresses from Gratuitous ARP responses.
Web Access Enabled	Indicates whether access to phone web pages is enabled (Yes) or disabled (No).
Settings Enabled	Indicates whether the Settings menu on the phone is accessible.
Security Mode	Indicates the security mode assigned to the phone
URL Information	
Information URL	URL of the help text that appears on the phone.

Table 9-2 Network Information Items (continued)

Item	Description
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.
Idle URL	Not used.
Idle URL Timer	Not used.
Proxy Server URL	Not used.
Authentication URL	URL that the phone uses to validate requests made to the phone web server.
Locale Information	
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.
User Locale Version	Version of the user locale loaded on the phone.
User Locale Char Set	Character set that the phone uses for the user locale.
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.
Network Locale Version	Version of the network locale loaded on the phone.

Device Information

The Device Information web page displays device settings and related information for the phone. [Table 9-3](#) 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 9-1, and then click the **Device** hyperlink under the information area.

Table 9-3 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
Directory Number	Directory number assigned to the phone
System Load ID	Identifier of the firmware running on the phone
Version	Version of the phone hardware
Serial Number	Serial number of the phone
Model Number	Model number of the phone

Table 9-3 *Device Information Area Items (continued)*

Item	Description
Message Waiting	Indicates if there is a voice message waiting on any line for this phone
UDI	Displays the following Cisco Unique Device Identifier (UDI) information about the phone: <ul style="list-style-type: none"> • Device Type—Indicates hardware type such as phone • Device Description—Displays the name of the phone associated with the model type. • Product Identifier—Specifies the phone model • Version Identifier—Represents the hardware version of the phone • Serial Number—Displays the phone's unique serial number
Time	Time from the Date/Time Group in Cisco Unified Communications Manager
TimeZone	Time zone obtained from the Date/Time Group in Cisco Unified Communications Manager
Date	Date obtained from the Date/Time Group in Cisco Unified Communications Manager
Hardware Revision	Version of the phone hardware
WLAN Regulatory Domain	Identifier for the wireless regulatory region in which this phone must operate
USB Vendor/Product ID	Unique code that identifies the phone as a Cisco Systems product
USB RNDIS Device Address	Manufacturer-assigned unique MAC address for the USB Remote Network Driver Interface Specification (RNDIS) for the phone
USB RNDIS Host Address	Manufacturer-assigned unique MAC address for the USB RNDIS for the host

Wireless LAN Statistics

The Wireless LAN Statistics section provides information about packets that have been received and transmitted by the phone. [Table 9-4](#) describes the statistics.

Table 9-4 *Wireless LAN Statistics Items*

Item	Description
Rx Statistics	
Rx OK Frames	Number of packets received successfully
Rx Error Frames	Number of packets received with errors
Rx Unicast Frames	Number of packets received that are unicast traffic
Rx Multicast Frames	Number of packets received that are multicast traffic

Table 9-4 *Wireless LAN Statistics Items (continued)*

Item	Description
Rx Broadcast Frames	Number of packets received that are broadcast traffic
Rx FCS Frames	Number of packets received frames checksum error
Rx Beacons	Number of received beacons
Association Rejects	Number of rejected association attempts
Association Timeouts	Number of failed association attempts due to timeout
Authentication Rejects	Number of authentication attempts that the AP rejected
Authentication Timeouts	Number of failed authentication attempts due to timeout
Tx Statistics (Best Effort)	
Tx OK Frames	Number of frames transmitted with successfully
Tx Error Frames	Number of frames transmitted with errors
Tx Unicast Frames	Number of frames transmitted that are unicast traffic
Tx Multicast Frames	Number of frames transmitted that are multicast traffic
Tx Broadcast Frames	Number of frames transmitted that are broadcast traffic
RTS Fail Counter	Number of RTS transmissions that did not result in transmitted frames
ACK Fail Counter	Number of failed acknowledgements by the AP
Retries Counter	Number of frames that were retransmitted
Multiple Retries Counter	Number of frames for which retransmission was attempted
Failed Retries Counter	Number of frames without acknowledgements
Tx Timeout Counter	Number of frames that could not be retransmitted due to timeout
Other Fail Counter	Number of frames with failed transmission due to other causes
Success Counter	Number of frames transmitted successfully
Max Retry Limit Counter	Number of times the maximum retry limit was reached
Tx Statistics (Voice)	
Tx OK Frames	Number of frames transmitted with successfully
Tx Error Frames	Number of frames transmitted with errors
Tx Unicast Frames	Number of frames transmitted that are unicast traffic
Tx Multicast Frames	Number of frames transmitted that are multicast traffic
Tx Broadcast Frames	Number of frames transmitted that are broadcast traffic
RTS Fail Counter	Number of RTS transmissions that did not result in transmitted frames
ACK Fail Counter	Number of failed acknowledgements by the AP
Retries Counter	Number of frames that were retransmitted
Multiple Retries Counter	Number of frames for which retransmission was attempted
Failed Retries Counter	Number of frames without acknowledgements
Tx Timeout Counter	Number of frames that could not be retransmitted due to timeout
Other Fail Counter	Number of frames with failed transmission due to other causes

Table 9-4 *Wireless LAN Statistics Items (continued)*

Item	Description
Success Counter	Number of frames transmitted successfully
Max Retry Limit Counter	Number of times the maximum retry limit was reached

Network Statistics

The Network Statistics section provides information about network traffic. [Table 9-5](#) describes the IP, TCP, and UDP traffic.

Table 9-5 *Network Statistics Screen Items*

Item	Description
IP Statistics	
IpInReceives	Number of input datagrams received from interfaces including those received in error
IpInHdrErrors	Number of input datagrams discarded due to errors in IP headers
IpInAddrErrors	Number of input datagrams discarded because IP address in header destination field was not valid
IpInForwDatagrams	Number of input datagrams that were forwarded to another IP destination
IpInUnknownProtos	Number of datagrams discarded because of an unknown or unsupported protocol
IpInDiscards	Number of input datagrams discarded for reasons other than errors, such as lack of buffer space
IpInDelivers	Number of input datagrams successfully delivered to IP user-protocols
IpInOutRequests	Number of IP datagrams supplied to IP in request for transmission; does not include IPForwDatagram count
IpInOutDiscards	Number of output datagrams discarded for reasons other than errors, such as lack of buffer space
IpInOutNoRoutes	Number of output datagrams discarded because no route found to transmit them to destination
IpInReasmTimeout	Maximum number of seconds which received fragments are held while awaiting reassembly
IpReasmReqds	Number of IP fragments received that need to be reassembled
IpInReasmOKs	Number of IP fragments successfully reassembled
IpInReasmFails	Number of IP fragment reassembly failures
IpInFragOK	Number of IP datagrams that have been successfully fragmented
IpInFragFails	Number of IP datagrams that were discarded because they could not be fragmented
IpInFragCreates	Number of IP datagram fragments generated

Table 9-5 Network Statistics Screen Items (continued)

Item	Description
TCP Statistics	
TcpRtoAlgorithm	Determines timeout value used for retransmitting unacknowledged octets
TcpRtoMin	Minimum value for retransmission timeout in milliseconds
TcpRtoMax	Maximum value for retransmission timeout in milliseconds
TcpMaxConn	Number limit for total TCP connections that are supported; if dynamic, displays value of -1
TcpActiveOpens	Number of times TCP connections made a transition to SYN-SENT state from CLOSED state
TcpPassiveOpens	Number of times TCP connections made a transition to SYN-RCVD state from LISTEN state
TcpAttemptFails	Number of times TCP connections made a transition to CLOSED state from SYN-SENT or SYN-RCVD state, plus number of times transitioned to LISTEN state from SYN-RCVD state
TcpEstablishResets	Number of times TCP connections made a transition to CLOSED state from either ESTABLISHED or CLOSE-WAIT state
TcpCurrEstab	Number of times TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT state
TcpInSegs	Number of segments received including those in error on current connections
TcpOutSegs	Number of segments sent including those on current connections; excludes segments containing only retransmit octets
TcpRetransSegs	Number of TCP segments transmitted containing previously transmitted octets
TcpInErrs	Number of segments with bad TCP checksum
TcpOutRsts	Number of TCP segments sent containing RST flag
UDP Statistics	
UdpInDatagrams	Number of UDP datagrams delivered to UDP users
UdpNoPorts	Number of received UDP datagrams for which there was not application at the destination port
UdpInErrors	Number of received UDP datagrams not delivered for reasons other than no application at port
UdpOutDatagrams	Number of datagrams sent

Stream Statistics

The Stream Statistics menu provides information about two types of streaming. The first stream is RTP Statistics and the second stream is Voice Quality Metrics. [Table 9-6](#) description each field displayed in the Stream Statistics window.

Table 9-6 Stream Statistics Items

Item	Description
RTP Statistics	
Domain Name	Domain of the phone
Remote Port	Port number of the destination
Local Port	Port number of the phone
Receiver Joins	Number of times the phone has started receiving a stream
Host Name	Host name for the phone
Sender Packets	Number of RTP voice packets transmitted since voice stream was opened Note 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.
Sender Tool	Type of audio encoding used for the stream: G.729, G.711 u-law, G.711 A-law, or Lin16k
Sender Report Time	Internal time stamp indicating when this streaming statistics report was generated
Receiver Octets	Total number of octets received by the phone
Receiver Lost Packets	Number of missing RTP packets (lost in transit)
Receiver Reports	Number of times this streaming statistics report has been accessed from the web page (resets when the phone resets)
Voice Quality Metrics	
MOS LQK	Score that is an objective estimate of the mean opinion score (MOS) for listening quality (LQK) that rates from 5 (excellent) to 1 (bad). This score is based on audible concealment events due to frame loss in the preceding 8-second interval of the voice stream. For more information, see the “Resolving Voice Quality and Roaming” section on page 10-8 Note The MOS LQK score can vary based on the type of codec that the Cisco Unified IP Phone uses.
Min MOS LQK	Lowest MOS LQK score observed from start of the voice stream
MOS LQK Version	Version of the Cisco proprietary algorithm used to calculate MOS LQK scores
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
Conceal Secs	Number of seconds that have concealment events (lost frames) from the start of the voice stream (includes severely concealed seconds)

Related Topic

- [Resolving Voice Quality and Roaming, page 10-8](#)



CHAPTER 10

Troubleshooting the Cisco Unified Wireless IP Phone 7925G

This chapter provides information that can assist you in troubleshooting your Cisco Unified Wireless IP Phone. It contains the following sections:

- [Resolving Startup and Connectivity Problems, page 10-1](#)
- [Resolving Voice Quality and Roaming, page 10-8](#)
- [General Troubleshooting Information, page 10-14](#)
- [Erasing the Local Configuration, page 10-18](#)

For additional troubleshooting information, you can refer to the *Cisco Unified Communications Manager Troubleshooting Guide*.

Resolving Startup and Connectivity Problems

After installing a Cisco Unified IP Phone 7960 in your network and adding it to Cisco Unified Communications Manager Administration, the phone should start up as described in the “[Understanding the Phone Startup Process](#)” section on page 3-17. If the phone does not start up properly, see the following sections for troubleshooting information:

- [Symptom: Incomplete Startup Process, page 10-1](#)
- [Symptom: No Association to Cisco Aironet Access Points, page 10-2](#)
- [Symptom: No Registration to Cisco Unified Communications Manager, page 10-3](#)

Symptom: Incomplete Startup Process

When an IP Phone connects to the wireless network, the phone should go through its normal startup process and the phone screen should display information. If the phone does not complete the startup process, the cause might be due to low RF signal strength, network outages, a dead battery in the phone, or the phone might not be functional.

To determine whether the phone is functional, follow these suggestions to systematically eliminate these potential problems:

1. Verify that the wired network is accessible by placing calls to and from other wired Cisco Unified IP Phones.
2. Verify that the wireless network is accessible:

- Power on another previously functional Cisco Unified Wireless IP Phone 7925G to verify that the access point is active.
 - Power on the wireless IP phone that will not start up and move to a different access point location that is known to be good.
3. Verify that the phone is receiving power:
 - If you see “Low Battery” on the phone screen, the battery might be dead.
 - Insert a new or fully charged battery in the wireless IP phone that will not start up.
 - If you are using the battery, try plugging in the external power supply instead.
 4. If the phone does not power up successfully, and never shows the Main screen, try using Recovery Mode:
 - Press both the Push to Talk button and the Speaker button and then press the Power-on button.
 - The phone goes into recovery mode and checks the integrity of the firmware files.
 - If error messages display indicating “recovery required,” then plug the USB cable into the phone and a PC. See [“Configuring the USB LAN on the PC” section on page 4-2](#).
 - Using a browser, access the web page for the phone. See [“Accessing the Phone Web Page” section on page 4-3](#) for instructions.
 - Go to the Phone Recovery section on the web page and upload a new Phone Software TAR file.

If, after attempting these solutions, the phone still does not start up, contact a Cisco technical support representative for additional assistance.

Symptom: No Association to Cisco Aironet Access Points

After the Greeting Message displays, if a phone continues to cycle through messages displaying on the phone screen, the phone is not associating with the access point properly. The phone cannot successfully start up unless it associates and authenticates with an access point.

Verifying Access Point Settings

The Cisco Unified Wireless IP Phone 7925G must first authenticate and associate with an access point before it can obtain an IP address. The phone follows this start up process with the access point:

1. Scans for an access point
2. Associates with an access point
3. Authenticates using a preconfigured authentication method (if configured, can use LEAP, EAP-FAST, Auto (AKM), or others)
4. Obtains an IP address

Check the SSID settings on the access point and on the phone to be sure the SSID matches.

Check the authentication type settings on the access point and on the phone to be sure authentication/encryption settings match.



Note If the message, “No Service - IP Config Failed,” DHCP failed because the encryption between the access point and phone do not match.

If using static WEP, check the WEP key on the phone to be sure it matches the WEP key on the access point. Reenter the WEP key on the phone to be sure it is correct.



Note If open authentication is set, the phone is able to associate to an access point although the WEP keys are incorrect or mismatched.

Error Messages During Authentication

If you see the following error messages, check these problems:

Authentication failed, No AP found

- Check if the correct authentication method and related encryption settings are enabled on the access point.
- Check that the correct SSID is entered on the phone.
- Check that the correct username and password are configured when using LEAP, EAP-FAST or Auto (AKM) authentication.
- If you are using A WPA Preshared key or WPA2 Preshared Key, check that you have the correct passphrase configured.
- You might need to enter the user name on the phone in the domain\username format when authenticating with a Windows domain.

EAP authentication failed

- If you are using EAP, you might need to enter the EAP user name on the phone in the *domain\username* format when authenticating with a Windows domain.
- Check that the correct EAP username and password are entered on phone.

AP Error—Cannot support all requested capabilities

On the access point, check that CKIP/CMIC is not enabled for the voice VLAN SSID. The Cisco Unified Wireless IP Phone 7925G does not support these features.

Symptom: No Registration to Cisco Unified Communications Manager

If a phone proceeds past the first stage (authenticating with access point), and, continues to cycle through the messages displaying on the phone screen, the phone is not starting up properly. The phone cannot successfully start up until it connects to the LAN and registers with a Cisco Unified Communications Manager server.

These sections can assist you in determining the reason that the phone is unable to start up properly:

- [Registering the Phone with Cisco Unified Communications Manager, page 10-4](#)
- [Checking Network Connectivity, page 10-4](#)
- [Verifying TFTP Server Settings, page 10-4](#)
- [Verifying IP Addresses, page 10-5](#)
- [Verifying DNS Settings, page 10-5](#)
- [Verifying Cisco Unified Communications Manager Settings, page 10-5](#)
- [Cisco Unified Communications Manager and TFTP Services are not Running, page 10-6](#)

- [Creating a New Configuration File](#), page 10-7

Registering the Phone with Cisco Unified Communications Manager

A Cisco Unified Wireless IP Phone 7925G 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. If you see the error message, “Registration Rejected,” review the information and procedures in the [“Adding Users to Cisco Unified Communications Manager” section on page 7-19](#) 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. (To determine the MAC address of a phone, see the [“Viewing Device Information” section on page 8-4](#).)

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 10-7](#) for assistance.

Checking Network Connectivity

If the network is down between the access point and the TFTP server or Cisco Unified Communications Manager, the phone cannot start up properly. Ensure that IP connectivity exists between the WLAN and the Cisco Unified Communications Manager and TFTP servers.

Verifying TFTP Server Settings

The Cisco Unified Wireless IP Phone 7925G uses the TFTP server setting to identify the primary TFTP server to use. If the TFTP server does not respond to the request, then the Communications Manager1 (CM1) shows as TFTP_AS_CM if the phone has not registered with Cisco Unified Communications Manager before.



Note If the phone has previously registered with Cisco Unified Communications Manager, the Cisco Unified Communications Manager list information is cached in memory. If TFTP fails, you must power cycle the phone to connect to the TFTP server.

The phone tries to create a TCP connection to the TFTP IP address and then to the gateway. If Cisco Unified Communications Manager service is not running on the TFTP server, or if SRST is not running on the gateway, the wireless IP phone may continually cycle while attempting to contact the identified TFTP server.

The Cisco Unified Wireless IP Phone 7925G does not cache the IP information passed from the DHCP server, so the TFTP request must be sent and responded to every time the phone power cycles.

If you have assigned a static IP address to the phone, you must manually enter this setting. See the [“Configuring IP Network Settings” section on page 4-23](#).

If you are using DHCP and Cisco Unified Communications Manager, Release 4.x, the phone obtains the address for the TFTP server from the DHCP server. Check the IP address configured in Option 150 or Option 66. Refer to *Configuring Windows 2000 DHCP Server for Cisco Unified Call Manager* available at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_tech_note09186a00800942f4.shtml

You can also enable the phone to use a static TFTP server. Such a setting is particularly useful if the phone was recently moved from one location to another.

For information about determining and changing TFTP server settings, see “Configuring IP Network Settings” section on page 4-23 or “Viewing the Current Configuration” section on page 8-12.

Verifying IP Addresses

You should verify the IP addressing for the Cisco Unified Wireless IP Phone 7925G. 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.



Note

When the wireless IP phone loses the RF signal (goes out of the coverage area), the phone will not release the DHCP server unless it reaches the time-out state.

Check for these problems:

- 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. If you are using a DHCP server, and the wireless IP phone gets a response from the DHCP server, the information is automatically configured. Refer to *Troubleshooting Switch Port Problems*, available at this URL: <http://www.cisco.com/warp/customer/473/53.shtml>
- IP Address, Subnet Mask, Primary Gateway—If you have assigned a static IP address to the phone, you must configure settings for these options. See the “Configuring IP Network Settings” section on page 4-23.

If you are using DHCP, check the IP addresses distributed by your DHCP server. Be aware of DHCP conflicts and duplicate IP addresses. 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>

For information about determining and changing IP addressing, see “Configuring IP Network Settings” section on page 4-23

Verifying DNS Settings

If you are using DNS to refer to Cisco Unified Communications Manager, you must ensure that you have specified a DNS server. You should also verify that there is a CNAME entry in the DNS server for the Cisco Unified Communications Manager system.

You must also ensure that DNS is configured to do reverse look-ups. The default setting on Windows 2000 is to perform forward-only look-ups.

For information about determining and changing DNS settings, see “Configuring IP Network Settings” section on page 4-23.

Verifying Cisco Unified Communications Manager Settings

The Cisco Unified Wireless IP Phone 7925G 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. Take one of these actions to verify Cisco Unified Communications Manager settings:

- On the Cisco Unified Wireless IP Phone 7925G, choose **Menu > Network Config > Current Configuration** and look at the **Communications Manager 1–4** options.
- If none of the Cisco Unified Communications Manager 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 10-4 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 might not be able to start up properly. However, in such situations, 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 Unified 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 Cisco Unified Communications Manager and TFTP services for Cisco Unified Communications Manager 5.0 or later, follow these steps:

Procedure

-
- Step 1** From Cisco Unified Communications Manager Administration for 5.0 or later, choose **Cisco Unified Serviceability** from the Navigation drop-down list.
 - Step 2** Choose **Tools > Control Center - Network Services** and click Go.
 - Step 3** Click
 - Step 4** 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 stop or start a service.
 - Step 5** 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**.

To start Cisco Unified Communications Manager and TFTP services for Cisco Unified Communications Manager 4.x, follow these steps:

Procedure

-
- Step 1** From Cisco Unified Communications Manager Administration for 4.x, choose **Applications > Cisco Unified Communications Manager Serviceability**.
 - Step 2** Choose **Tools > Control Center**.
 - Step 3** From the Servers column, choose the primary Cisco Unified Communications Manager server.

The page displays the service names for the server that you chose, the status of the services, and a service control panel to stop or start a service.

Step 4 If a service has stopped, click the **Start** button.

The Service Status symbol changes from a square to an arrow.

**Note**

For more information, see the *Cisco Unified Communications Manager Administration Guide* and the *Cisco Unified Serviceability Administration Guide*.

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 might be corrupted.

To create a new configuration file, follow these steps:

Procedure

- Step 1** From Cisco Unified Communications Manager, select **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 Users to Cisco Unified Communications Manager”](#) section on page 7-19 for details.
 - Step 4** Power cycle the wireless IP phone.
-

**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 directory number (DN) remains in the Cisco Unified Communications Manager database as an unassigned DN. You can assign these DNs to other devices or 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.

Related Topics

- [Resolving Startup and Connectivity Problems, page 10-1](#)
- [Resolving Voice Quality and Roaming, page 10-8](#)
- [General Troubleshooting Information, page 10-14](#)

Resolving Voice Quality and Roaming

Cisco Unified Wireless IP Phone 7925G users might have problems with voice quality and connectivity when roaming with their phones. See the following sections for troubleshooting information:

- [Symptom: Cisco Unified Wireless IP Phone Resets Unexpectedly, page 10-8](#)
- [Symptom: Audio Problems, page 10-10](#)
- [Symptom: Improper Roaming and Voice Quality or Lost Connection, page 10-11](#)
- [Monitoring the Voice Quality of Calls, page 10-12](#)

Symptom: Cisco Unified Wireless IP Phone Resets Unexpectedly

If users report that their phones are resetting during calls or resetting 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 Wireless IP Phone 7925G should not reset on its own.

Typically, a phone resets if it has problems connecting to the access point and LAN or to Cisco Unified Communications Manager. These sections can help you identify the cause of a phone resetting in your network:

- [Verifying Access Point Settings, page 10-8](#)
- [Identifying Intermittent Network Outages, page 10-8](#)
- [Verifying DHCP Settings, page 10-9](#)
- [Verifying Voice VLAN Configuration, page 10-9](#)
- [Verifying that the Phones Have Not Been Intentionally Reset, page 10-9](#)
- [Eliminating DNS or Other Connectivity Errors, page 10-9](#)

Verifying Access Point Settings

Verify that the wireless configuration is correct. For example, check if the particular access point or switch to which the phone is connected is down. See the [“VoIP WLAN Configuration” section on page 2-21](#) for information about access point settings.

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. The phone can retransmit and attempt to recover, or if the phone reaches the maximum retransmit rate, it drops the packets or loses association with the access point.

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

Verifying DHCP Settings

To determine if the phone has been properly configured to use DHCP, follow these steps:

-
- Step 1** Verify that you have properly configured the phone to use DHCP. See the [“Configuring DHCP Settings” section on page 5-6](#) for details.
 - Step 2** Verify that the DHCP server has been set up properly.
 - Step 3** Verify the DHCP lease duration. Your local policy determines this setting.

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.

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 access point and switch as phone), it is likely that you do not have a voice VLAN or the appropriate QoS settings configured.

By isolating the wireless phones on a separate auxiliary VLAN, you can use QoS to prioritize the voice traffic over data traffic and improve the voice quality. See the [“Voice QoS in a Wireless Network” section on page 2-12](#) 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.

Eliminating DNS or Other Connectivity Errors

If the phone does not register with Cisco Unified Communications Manager, check to see if you are using host names or IP addresses for Cisco Unified Communications Manager servers.

To eliminate DNS or other connectivity errors, follow these steps:

Procedure

- Step 1** Reset the phone to factory defaults. See the [“Erasing the Local Configuration” section on page 10-18](#) for details.
- Step 2** Modify DHCP and IP settings:
 - a. Disable DHCP. See the [“Configuring DHCP Settings” section on page 5-6](#) for details.
 - b. Assign static IP values to the phone. See the [“Configuring DHCP Settings” section on page 5-6](#) for details. Use the same default router setting used for other functioning Cisco Unified IP Phones.

- c. Assign a TFTP server. See the “[Configuring an Alternate TFTP Server](#)” section on page 5-7 for details. Use the same TFTP server used for other functioning Cisco Unified IP Phones.

Step 3 From Cisco Unified Communications Manager, choose **System > Server** and verify that the server is referred to by its IP address and not by its host name.



Note Cisco recommends that you configure IP addresses only and not host names to eliminate the DNS resolution in the phone registration process.

Step 4 From Cisco Unified Communications Manager, select **Device > Phone** and verify that you have assigned the correct MAC address to this Cisco Unified IP Phone.

To determine the MAC address of a phone, see the “[Viewing Device Information](#)” section on page 8-4.

Step 5 Power cycle the phone.

Symptom: Audio Problems

When users report that active phone calls have poor voice quality that includes choppy audio, static or gaps in audio, or no audio, you can use the following suggestions to identify the cause of the problem.

These sections can assist you with the following symptoms:

- [No Audio During a Connected Call](#), page 10-10
- [One-Way Audio During a Connected Call](#), page 10-10

No Audio During a Connected Call

If you are using a release earlier than 2.0, then you must disable TKIP and MIC features on the access point. These features are only supported with release 2.0 and later on the Cisco Unified Wireless IP Phone 7925G.

One-Way Audio During a Connected Call

Use the following list to identify possible causes for the problem:

- Check the access point to see that the transmit power setting matches the transmit power setting on the phone. One-way audio is common when the access point power setting is greater (100mW) than that of the phone (20mW).

Cisco Unified Wireless IP Phone 7925G Firmware supports dynamic transmit power control (DTPC). The phone uses the transmit power that the access point advertises upon association.



Note With DTCP, if Client Transmit Power is set in the access point, the phone automatically uses the same client power setting. If the access point is set for the maximum setting (Max), the access point uses the Transmit Power setting on the phone.

- Check that the access point is enabled for ARP caching. When the Cisco Unified Wireless IP Phone 7925G is in power save mode or scanning, the access point can respond to the wireless IP phone only when ARP caching is enabled.

See the “[VoIP WLAN Configuration](#)” section on page 2-21 for more information.

- Check your gateway and IP routing for voice problems.
- Check if a firewall or NAT is in the path of the RTP packets. If so, you can use Cisco IOS and PIXNAT to modify the connections so that two-way audio is possible.
- Check that the Data Rate setting for the phone and the access point are the same. These settings should match or the phone should be set for Auto.
- Check the phone hardware to be sure the speaker is functioning properly.
- Check the volume settings in the Phone Settings menu.

Symptom: Improper Roaming and Voice Quality or Lost Connection

If users report that when engaged in an active phone call and walking from one location to another (roaming), the voice quality deteriorates or the connection is lost, you can use the following suggestions to identify the cause of the problem.

These sections can assist you with the following symptoms:

- [Voice Quality Deteriorates While Roaming](#), page 10-11
- [Delays in Voice Conversation While Roaming](#), page 10-11
- [Phone Loses Connection with Cisco Unified Communications Manager While Roaming](#), page 10-11
- [Phone Does Not Roam Back to Preferred Band](#), page 10-12

Voice Quality Deteriorates While Roaming

Check the RSSI on the destination access point to see if the signal strength is adequate. The next access point should have an RSSI value of -67 dBm or greater.

Check the site survey to determine if the channel overlap is adequate for the phone and the access point to hand off the call to the next access point before the signal is lost from the previous access point.

Check to see if noise or interference in the coverage area is too great.

Check that signal to noise ratio (SNR) levels are 25 db or higher for acceptable voice quality.

Delays in Voice Conversation While Roaming

Use the Site Survey Utility on the Cisco Unified Wireless IP Phone 7925G to see if there is another acceptable access point as a roaming option. The next access point should have an RSSI value of 35 or greater to roam successfully.

Check the Cisco Catalyst 45xx switch to see if it has the correct version of Supervisor (SUP) blades. The blades must be versions SUP2+ or higher to prevent roaming delays.

Phone Loses Connection with Cisco Unified Communications Manager While Roaming

Check for the following configuration or connectivity issues between the phone and the access point:

- The RF signal strength might be weak. Use the Site Survey Tool and check the RSSI value for the next access point.
- The next access point might not have connectivity to Cisco Unified Communications Manager.

- There might be an authentication type mismatch between the phone and the next access point.
- The access point might be in a different subnet from the previous access point. The Cisco Unified Wireless IP Phone 7925G is capable of Layer 2 roaming only. Layer 3 roaming requires WLSM that uses GRE. For more information, see [“WLANs and Roaming” section on page 2-7](#).
- If using EAP-FAST, LEAP, or Auto (AKM) authentication, the access point might be using filters to block TCP ports. The ACS server uses port 1645 for authentication and 1646 for accounting and the RADIUS server uses port 1812 for authentication and 1813 for accounting.

Phone Does Not Roam Back to Preferred Band

When the Cisco Unified IP Phone 7960 is set to 5 GHz band as the preferred network and is authenticated to an AP on that band and roams to an area in which 5 GHz is not longer available but 2.4 GHz is available, the phone operates. But if you roam back to the 5 GHz band area, the phone will not return to the 5GHz band.

Since the phone will only switch between bands when connectivity has been lost, you must reboot the phone to return to the preferred band of 5 GHz.

Related Topics

- [Resolving Startup and Connectivity Problems, page 10-1](#)
- [Resolving Voice Quality and Roaming, page 10-8](#)
- [General Troubleshooting Information, page 10-14](#)
- [Monitoring the Voice Quality of Calls, page 10-12](#)

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, Cisco Voice Transmission Quality (CVTQ) index. Depending on the MOS LQK version number, these scores might be compliant with the International Telecommunications Union (ITU) standard P.564. This standard defines evaluation methods and performance accuracy targets that predict listening quality scores based on observation of actual network impairment.

**Note**

Concealment ratio and concealment seconds are primary measurements based on frame loss while MOS LQK scores project a “human-weighted” version of the same information on a scale from 5 (excellent) to 1 (bad) for measuring listening quality.

Listening quality scores (MOS LQK) relate to the clarity or sound of the received voice signal. Conversational quality scores (MOS CQ such as G.107) include impairment factors, such as delay, that degrade the natural flow of conversation.

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 remotely by using Streaming Statistics (see [Chapter 9, “Monitoring the Cisco Unified Wireless IP Phone Remotely.”](#))

Using Voice Quality Metrics

To use the metrics for monitoring voice quality, note the typical scores under normal conditions of zero packet loss, and use the metrics as a baseline for comparison.

It is important to distinguish significant changes from random changes in metrics. Significant changes are scores that change about 0.2 MOS or greater and persist in calls that last longer than 30 seconds. Conceal Ratio changes should indicate greater than 3 percent frame loss.

MOS LQK scores can vary based on the codec that the Cisco Unified IP Phone uses. The following codecs provide these maximum MOS LQK scores under normal conditions with zero frame loss:

- G.711 codec gives 4.5 score
- G.729A/ AB gives 3.7 score

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

Troubleshooting Tips

When you observe significant and persistent changes to metrics, use [Table 10-1](#) for general troubleshooting information.

Table 10-1 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"> • Average MOS LQK decreases could indicate widespread and uniform impairment. • Individual MOS LQK decreases indicate bursty impairment. <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"> • Check to see if the phone is using a different codec than expected (RxType and TxType). • Check to see if the MOS LQK version changed after a firmware upgrade.

Table 10-1 Changes to Voice Quality Metrics (continued)

Metric Change	Condition
Conceal Ratio and Conceal Seconds increase significantly	<ul style="list-style-type: none"> Network impairment from packet loss or high jitter.
Conceal Ratio is near or at zero, but the voice quality is poor	<ul style="list-style-type: none"> Noise or distortion in the audio channel such as echo or audio levels. Tandem calls that undergo multiple encode/decode such as calls to a cellular network or calling card network. Acoustic problems coming from a speakerphone, handsfree cellular phone or wireless headset. <p>Check packet transmit (TxCnt) and packet receive (RxCnt) counters to verify that voice packets are flowing.</p>

**Note**

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

General Troubleshooting Information

The following topics provide general information and tips for troubleshooting the Cisco Unified Wireless IP Phone 7925G.

- [Common Phone Status Messages, page 10-14](#)
- [Troubleshooting Tips for the Cisco Unified Wireless IP Phone 7925G, page 10-16](#)
- [Logging Information for Troubleshooting, page 10-17](#)

Common Phone Status Messages

[Table 10-2](#) provides a list of common status messages that display on the phone screen. The table provides possible causes and recommended actions to assist with troubleshooting the problem.

Table 10-2 Common Phone Status Messages

Message	Description	Possible Explanation and Action
Network Busy	The phone is unable to complete a call.	The WLAN is not able to allocate bandwidth for the phone to complete the call. Wait a few minutes and try the call again. If the problem persists, the WLAN might be congested. Consider increasing the WLAN bandwidth.
Leaving Service Area	The phone is unable to place or receive calls. The no signal icon displays on the phone screen.	<ul style="list-style-type: none"> The phone cannot detect any access point (AP) beacons. The phone is out of range of all APs. Move to a location that is within the coverage area. The AP has failed. Run diagnostic tests on the AP and replace if defective.
Locating Network Services	The phone is searching for an AP.	The phone is searching all beacons and scanning for a channel and SSID to use. Wait for the phone to complete the searching and scanning process. Depending on the signal strength of the available WLAN, this process can take a few minutes.
Authentication Failed	The phone is unable to access the WLAN, and the main phone screen is not active.	The authentication server does not accept the security credentials. Verify that the security mode and credentials are correct by viewing the Network profile. For information about accessing and changing Network profiles, see the “Accessing a Network Profile” section on page 5-3.
Configuring IP	The main phone screen is not active.	The phone is attempting to obtain network parameters such as its IP address, or the IP address of the gateway or router from the DHCP server. Wait a few minutes for the phone to obtain the network parameters. If the phone unable to retrieve the IP address, then check that the DHCP server is up and running.
Configuring CM List	The main phone screen is not active.	The phone is downloading its configuration files from the TFTP server. Wait a few minutes for the phone to download all of its configuration files.

Troubleshooting Tips for the Cisco Unified Wireless IP Phone 7925G

Table 10-3 provides general troubleshooting information for the wireless IP phone.

Table 10-3 Cisco Unified Wireless IP Phone Troubleshooting Tips

Summary	Explanation
Phone is resetting	<p>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 access point problems, switch outages, and switch reboots.</p> <p>See the “Symptom: Cisco Unified Wireless IP Phone Resets Unexpectedly” section on page 10-8.</p>
Time on phone is incorrect	<p>Sometimes the time or date on the phone is incorrect. The Cisco Unified Wireless IP Phone 7925G gets its time and date when it registers with Cisco Unified Communications Manager. Power cycle the phone to reset the time or date.</p> <p>The time shows in either 12 hour or 24 hour format.</p>
Ring volume is too low	<p>To see if the ring volume is set correctly on the phone, choose Settings > Phone Settings > Sound Settings > Volumes. Scroll up for the highest volume</p> <p>You can also press the volume button on the side of the phone and the volume setting appears on the phone screen.</p>
Phone does not ring	<p>To see if the phone is set to ring, choose Settings > Phone Settings > Sound Settings > Alert Pattern, and check that it a ring setting is selected.</p> <p>To see if a ring tone has been set for the phone, choose Settings > Phone Settings > Ring Tone. If none is set, add a ring tone for the phone.</p> <p>To see if the speaker is functioning properly, adjust the ring volume settings to the highest level. Enable keypad tones or call the phone to check the speaker.</p>
One-way audio on phone	<p>Check that the speaker is functioning properly. Adjust the speaker volume setting and call the phone to check the speaker.</p> <p>Check that ARP caching has been set on the AP. See “VoIP WLAN Configuration” section on page 2-21.</p>
Delays when roaming from one location to another	<p>If Cisco Catalyst 45xx series switches are being used as the main Layer 3 switches in the network, ensure that the supervisor blades are a minimum SUP2+ or later version. The Cisco Unified Wireless IP Phone 7925G (or any wireless client) experiences roaming delays when an earlier version (SUP 1 or SUP2) blade is used.</p>
Phone firmware downgrades	<p>After applying a Cisco Unified Communications Manager upgrade or patch, that is older than the current Cisco Unified Wireless IP Phone 7925G firmware, the phones could automatically downgrade to the load contained in the patch. Check the Cisco Unified Communications Manager 7925G device default image in the TFTP folder to fix this problem.</p>

Table 10-3 Cisco Unified Wireless IP Phone Troubleshooting Tips (continued)

Summary	Explanation
Battery life is shorter than specified	<p>An unstable RF environment can cause the phone to remain in active mode because it is constantly seeking an AP. This reduces the battery life considerably. When leaving an area of coverage, shut down the phone.</p> <p>Higher phone transmit power can affect battery life.</p> <p>To maximize idle time on the phone and conserve battery life, you need to optimize the registration time so the phone can go into power save mode more often.</p>
Phone call cannot be established	<p>The phone does not have a DHCP IP address, is unable to register to Cisco Unified Communications Manager, and shows a Configuring IP or Registering message.</p> <p>Verify the following:</p> <ol style="list-style-type: none"> 1. The Cisco Unified Communications Manager service is running on the Cisco Unified Communications Manager server. 2. Both phones are registered to the same Cisco Unified Communications Manager. 3. Audio server debug and capture logs are enabled for both phones. If needed, enable Java debug.
Call established with the iLBC protocol does not show that the iLBC codec is being used	<p>Call statistics display does not show iLBC as the receiver/sender codec.</p> <ol style="list-style-type: none"> 1. Check the following using the Cisco Unified Communications Manager administration pages: <ul style="list-style-type: none"> – Both phones are in the iLBC device pool. – The iLBC device pool is configured with the iLBC region. – The iLBC region is configured with the iLBC codec. 2. Capture a sniffer trace between the phone and Cisco Unified Communications Manager and verify that SCCP messages, OpenReceiveChannel, and StationMediaTransmit messages have media payload type value equal to 86. If so, the problem is with the phone; otherwise the problem is with the Cisco Unified Communications Manager configuration. 3. Enable audio server debug and capture logs from both phones. If needed, enable Java debug.

Related Topics

- [Logging Information for Troubleshooting, page 10-17](#)
- [General Troubleshooting Information, page 10-14](#)

Logging Information for Troubleshooting

The following options can help you gather troubleshooting information:

- [Using a System Log Server, page 10-18](#)
- [Using the Trace Logs on the Unified IP Phone, page 10-18](#)

Using a System Log Server

To gather information about problems with the wired network that can cause roaming delays or no connectivity, set up a system log server. Enable “syslog” on the network switches and access points that is logged to the system log server. Also enable Network Time Protocol (NTP) so that all access points and switches use the same times.

For information about setting up a system log server, see [“Configuring Trace Settings” section on page 4-27](#).

Using the Trace Logs on the Unified IP Phone

When you are experiencing problems with registering with Cisco Unified Communications Manager, or call connections, you can use this function to trace the path of a packet from the phone to Cisco Unified Communications Manager. The result shows the number of hops and the IP address of each hop to reach the Cisco Unified Communications Manager server. You can use this information to check connectivity between the phone, Cisco Unified Communications Manager servers and gateways during a call.

To download trace logs, click **Download Logs** from the Trace Logs page.

For information, see the [“Viewing Trace Logs” section on page 4-34](#).

Internet Explorer Error When Downloading Trace Logs

Depending on your settings, Internet Explorer might display an error when you download a trace log from the Trace Logs page.

To prevent this error from displaying, follow these steps:

Procedure

-
- Step 1** From Internet Explorer, choose **Tools > Internet Options**.
 - Step 2** In the Internet Options window, click the Advanced tab.
 - Step 3** Under the Security section, enable Do not save encrypted pages to disk, and click **OK**.
 - Step 4** Quit all Internet Explorer sessions.
-

Related Topics

- [Resolving Startup and Connectivity Problems, page 10-1](#)
- [Resolving Voice Quality and Roaming, page 10-8](#)
- [Erasing the Local Configuration, page 10-18](#)

Erasing the Local Configuration

You can clear all locally stored configuration options in a phone by using the Phone Settings menu. When you use the restore to factory default option, all user-defined entries in Network Profiles, Phone Settings, and Call History are erased.

To erase the local configuration, follow these steps:

Procedure

- Step 1** Choose **SETTINGS > Phone Settings**.
- Step 2** Press ****2** on the keypad.
The phone briefly displays “Start factory reset now?”
- Step 3** Press the **Yes** softkey. All settings are deleted.
The phone cycles through normal startup procedures.
Or press **No** to cancel the reset.
- Step 4** Press **SETTINGS > Network Profiles** to reconfigure the network settings for your WLAN.
-



Caution

Erasing the local configuration removes network profiles that are set up for the Cisco Unified Wireless IP Phone to access the WLAN. You must reconfigure the network settings after performing the reset to enable the phone to access the WLAN.

Related Topics

- [Resolving Startup and Connectivity Problems, page 10-1](#)
- [Resolving Voice Quality and Roaming, page 10-8](#)
- [General Troubleshooting Information, page 10-14](#)



APPENDIX **A**

Providing Information to Users By Using 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.

To successfully use some features on the Cisco Unified Wireless IP Phone 7925G (such as speed dial numbers and voice messaging system options), users must receive information from you or your network team or be able to contact you for assistance.

Cisco recommends that you create a web page on your internal support site that provides end users with important information about their new Cisco Unified Wireless IP Phone 7925G.

Consider adding the following types of information to this site:

- [How the Cisco Unified Wireless IP Phone Operates, page A-1](#)
- [How to Care for and Clean the Phone, page A-2](#)
- [How Users Access the Help System on the Phone, page A-3](#)
- [How Users Get Copies of Cisco Unified IP Phone Manuals, page A-3](#)
- [How Users Configure Phone Features and Services, page A-4](#)
- [How Users Access Voice Messages, page A-4](#)

How the Cisco Unified Wireless IP Phone Operates

Users need to know that their Cisco Unified Wireless IP Phone 7925G operates more like a cell phone than like their desktop phone. Small wireless phones with an antenna allow users to move around a facility while staying connected to a call. These phones, like cell phones, can approach the edge of the RF signal range and experience static or poor voice quality. At times, the user might encounter areas where there is no signal and lose the call entirely. The following is a list of calling locations and situations in which wireless phones might experience audio problems:

- Stairwells, elevators, rooms with metal equipment such as file cabinets, or heavy machinery
- Break rooms with microwave ovens, or labs with equipment that emits RF signals within the same ranges.
- Conference rooms or other congested areas where many people are using wireless devices
- Parking garages and outdoor areas where access points are not located or out of range.

**Caution**

This product is not a medical device and may use an unlicensed frequency band that is susceptible to interference from other devices or equipment.

The Cisco Unified Wireless IP Phone 7925G has many of the same phone features as the IP phone desktop models, such as Mute, access to voice messaging, and directories. The phone has a limited number of buttons, because of its size. As a consequence, the following are some differences in its operation:

- No line buttons—You must enter the phone number from the key pad and press Send. You can press the Phone icon from the main screen to use other lines on your phone.
- Only two softkeys—You must press the Options softkey to see the list of softkey features.
- You do not hear a dial tone.

Related Topics

- [How to Care for and Clean the Phone, page A-2](#)
- [How Users Get Copies of Cisco Unified IP Phone Manuals, page A-3](#)
- [How Users Configure Phone Features and Services, page A-4](#)
- [How Users Access Voice Messages, page A-4](#)

How to Care for and Clean the Phone

Users need to know how to protect and clean their phone. These guidelines provide information about using accessories and cleaning the Cisco Unified Wireless IP Phone 7925G:

- Use only chargers, batteries, and accessories that are approved by the Cisco Unified Wireless IP Phone 7925G manufacturer. Use of unapproved chargers, batteries, and accessories might be dangerous.
- Do not adhere a clip to the back of the phone or insert a clip between the phone and battery cover because it can damage the battery.
- When disconnecting the power cord of any accessory, grasp and pull the plug. Do not pull the cord.
- Keep accessories out of reach of young children.
- Clean the phone with any moist wipe.

**Note**

Using unapproved accessories, not protecting the phone from moisture, contaminants, and hard impacts can invalidate the one-year hardware warranty.

For a list of available accessories and their descriptions, refer to the *Cisco Unified Wireless IP Phone 7925G Accessory Guide* at this URL:

http://www.cisco.com/en/US/products/hw/phones/ps379/products_user_guide09186a008076b878.html

Related Topics

- [How the Cisco Unified Wireless IP Phone Operates, page A-1](#)
- [How Users Access the Help System on the Phone, page A-3](#)
- [How Users Get Copies of Cisco Unified IP Phone Manuals, page A-3](#)

- [How Users Configure Phone Features and Services, page A-4](#)
- [How Users Access Voice Messages, page A-4](#)

How Users Access the Help System on the Phone

This Cisco Unified Wireless IP Phone 7925G provides access to a comprehensive online help system. To view the main help menu on a phone, from the main screen, press the Select button in the center of the navigation button. Wait for several seconds for this menu to appear.

- About Your Cisco Unified IP Phone—Details about your phone
- How do I...?—Procedures for common phone tasks
- Calling Features—Descriptions and procedures for calling features
- Help—Tips on using and accessing Help
- [How the Cisco Unified Wireless IP Phone Operates, page A-1](#)
- [How to Care for and Clean the Phone, page A-2](#)
- [How Users Get Copies of Cisco Unified IP Phone Manuals, page A-3](#)
- [How Users Configure Phone Features and Services, page A-4](#)
- [How Users Access Voice Messages, page A-4](#)

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. This documentation includes detailed user instructions for key phone features. See the “[Related Documentation](#)” section on page xiii for more information.

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

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

For more information about viewing or ordering documentation, see [Obtaining Documentation and Submitting a Service Request, page -xiii](#).

Related Topics

- [How the Cisco Unified Wireless IP Phone Operates, page A-1](#)
- [How to Care for and Clean the Phone, page A-2](#)
- [How Users Access the Help System on the Phone, page A-3](#)
- [How Users Configure Phone Features and Services, page A-4](#)
- [How Users Access Voice Messages, page A-4](#)

How Users Configure Phone Features and Services

End users can perform a variety of activities using the Cisco Unified Communications Manager User Options web page. Cisco Unified Wireless IP Phone users can set up speed dial and call forwarding numbers. Keep in mind that configuring settings on a phone 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 page.

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

- The URL required to access the application. This URL is:
`https://server_name:port_number/ccmuser/`
where *server_name* is the host on which the web server is installed, and *port_number* is the port address.
- A user ID and default password for accessing 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 7-19).
- A description of a web-based, graphical user interface application and how to access it with a web browser.
- An overview of tasks that users can accomplish by using the web page.

You can refer users to *Customizing Your Cisco Unified IP Phone on the Web*, for Cisco Unified Communications Manager Release 4.x, at

http://www.cisco.com/en/US/docs/voice_ip_comm/cuipph/all_models/4_1_user_options/english/user/guide/usopt.pdf

Related Topics

- [How the Cisco Unified Wireless IP Phone Operates, page A-1](#)
- [How to Care for and Clean the Phone, page A-2](#)
- [How Users Access the Help System on the Phone, page A-3](#)
- [How Users Get Copies of Cisco Unified IP Phone Manuals, page A-3](#)
- [How Users Access Voice Messages, page A-4](#)

How Users Access Voice Messages

Cisco Unified Communications Manager provides the flexibility to integrate with many different voice messaging systems, including the Cisco Unity voice messaging system. Because you can integrate with many different systems, you must provide users with detailed information about how to use your specific system.

You should provide this information to each user:

- How to access the voice messaging system account.
- The 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 messages are waiting.

Make sure that you have used Cisco Unified Communications Manager to set up a message waiting indicator (MWI) method.

For information about setting up the MWI method and the interface to the voice messaging system in Cisco Unified Communications Manager, refer to the documentation for your system at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

If you are using a Cisco Unity voice messaging system, refer to the Cisco Unity documentation for your system for configuring voice messaging and the initial passwords at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/tsd_products_support_series_home.html

Refer to the *Cisco Unified Wireless IP Phone 7925G Guide* for information about accessing the voice messaging system from the phone at this URL:

http://www.cisco.com/en/US/products/hw/phones/ps379/products_user_guide_book09186a008076b8af.html

Related Topics

- [How the Cisco Unified Wireless IP Phone Operates, page A-1](#)
- [How to Care for and Clean the Phone, page A-2](#)
- [How Users Access the Help System on the Phone, page A-3](#)
- [How Users Get Copies of Cisco Unified IP Phone Manuals, page A-3](#)
- [How Users Configure Phone Features and Services, page A-4](#)



APPENDIX **B**

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, see the “[Installing the Cisco Unified Communications Manager Locale Installer](#)” section on page B-1 to ensure that the phones are set up properly for your users.

Prior to deploying the wireless IP phones, download the locale installer for the firmware releases and configure the languages in Cisco Unified Communications Manager.

You can obtain translated documentation for the Cisco Unified IP Phones at this URL:

http://www.cisco.com/en/US/products/hw/phones/ps379/tsd_products_support_translated_end_user_guides_list.html

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 must install the locale-specific version of 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. You can find locale-specific versions of the Cisco Unified Communications Manager Locale Installer at

<http://www.cisco.com/kobayashi/sw-center/telephony/callmgr/locale-installer.shtml>.

For more information, refer to the “Locale Installation” section in the *Cisco Unified Communications Platform Administration Guide*.



Note

All languages may not be immediately available, so continue to check the website for updates.

Support for International Call Logging

If your phone system is configured for international call logging, the call logs, redial, or call directory entries may display a “+” symbol to represent the international escape code for your location. Depending on the configuration for your phone system, the “+” may be replaced with the correct international dialing code, or you may need to edit the number before dialing to manually replace the “+” with the international escape code for your location. In addition, while the call log or directory entry may display the full international number for the received call, the phone display may show the shortened local version of the number, without international or country codes.



APPENDIX C

Physical and Operating Environment Specifications

The following section describes the technical specifications for the Cisco Unified Wireless IP Phone 7925G. [Table C-1](#) shows the physical and operating environment specifications.

Table C-1 *Physical and Operating Environmental Specifications*

Specification	Value or Range
Operating Temperature	0° to 40°C (32° to 104°F)
Operating Relative Humidity	10% to 95% (non-condensing)
Storage Temperature	-30° to 60°C (-22° to 140°F)
Drop Specification	5 ft (1.5 m) to concrete without carrying case
Thermal Shock	-22°F (-30° C) for 24 hours to up to 158°F (+70°C) for 24 hours
Vibration	1.5 Grms maximum, 0.1 in. (2.5 mm) double amplitude at 0.887 octaves per minute from 5-500-5 Hz sweep; 10-minute dwell on three major peaks in each of the three major mutually perpendicular axis
Altitude	Certified for operation from 0 to 6,500 ft (0 to 2km)
Endurance	IP54; MIL810F
Phone Height	5.0 in. (12.7 cm)
Phone Width	2.0 in. (5.2 cm)
Phone Depth	0.8 (2.0 cm)
Phone Weight	4.8 to 5.0 oz. (138 to 143 g) ¹
LCD	2 inches wide with 176 by 220 pixel resolution
Power	AC adapters by geographic region

1. Depends on the weight of the battery pack.



APPENDIX **D**

Checklist for Deploying the Cisco Unified Wireless IP Phone 7925G

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

- [Configuring a Wireless Network, page D-1](#)
- [Configuring QoS Policies, page D-3](#)
- [Configuring the Cisco Unified Wireless IP Phone 7925G in Cisco Unified Communications Manager, page D-4](#)
- [Installing the Cisco Unified Wireless IP Phone 7925G, page D-7](#)

Configuring a Wireless Network

[Table D-1](#) explains and provides references for many of the configuration activities for the Cisco Aironet Access Point, controller, and Ethernet switch.



Note

When deploying the Cisco Unified Wireless IP Phone 7925G with World regulatory domain (CP-7925GW-K9), you must enable the access points for world mode (802.11d). The world model phone gets the channels and power information from the access point.

Table D-1 **Wireless Network Configuration Tasks**

Activity	Explanation	Reference
1. Check that the Cisco IOS version is the recommended version	<ul style="list-style-type: none">• Under System Software, verify that Cisco IOS version 12.3(8)JA or later is running on the AP.• For the controller, use Version 4.0 and Cisco IOS version 12.3(8)JX or later.	Components of the VoIP Wireless Network, page 2-9
2. Configure a VLAN for voice	Isolate voice traffic and enable QoS by configuring a separate voice VLAN on the access point and network switch.	Voice QoS in a Wireless Network, page 2-12 Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, Cisco IOS Release 12.3(8)JA

Table D-1 Wireless Network Configuration Tasks (continued)

Activity	Explanation	Reference
3. Configure Service Set Identifier (SSID) for each VLAN	Configure an SSID for a set of wireless devices to communicate with each other. Several access points can have the same SSID to support a group of wireless phones.	Associating to APs, page 2-12 <i>Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, Cisco IOS Release 12.3(8)JA</i>
4. Configure QoS settings for VLANs	<ul style="list-style-type: none"> a. Create a QoS policy for the voice VLAN and assign a higher CoS to voice traffic. b. Enable the QoS element for wireless IP phones to provide channel utilization (QBSS) information to phones. 	Voice QoS in a Wireless Network, page 2-12 Configuring QoS Policies, page D-3 <i>Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, Cisco IOS Release 12.3(8)JA</i>
5. Enable ARP caching	Enable this option to ensure two-way audio. The access point has ARP caching disabled by default.	<i>Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, Cisco IOS Release 12.3(8)JA</i>
6. Configure radio (802.11) settings	<ul style="list-style-type: none"> • Data Rate—Set for 11 Mbps or to the rate for the frequency band that you are using. • Client Transmit Power—After a site survey, determine the appropriate power requirements and set a specific Client Transmit Power setting. The Cisco Unified Wireless IP Phone 7925G uses the same setting as the access point. <p>Note If set for Max, the access point does not advertise Client Transmit Power setting.</p>	<i>Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, Cisco IOS Release 12.3(8)JA</i> <i>Cisco Unified Wireless IP Phone 7925G Deployment Guide</i>
7. Configure Security for the voice VLANs	Use one of these authentication and encryption options for the SSID that corresponds to the voice VLAN: <ul style="list-style-type: none"> • Open • Shared Key • EAP • Auto (AKM) 	Interacting with Cisco Unified Communications Manager, page 2-14 <i>Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, Cisco IOS Release 12.3(8)JA</i>

Configuration Tip for Cisco Aironet Access Points

If you are using EAP-FAST, you must increase the EAP request (802.1x) timeout to at least 20 seconds to ensure that the phone gets the PAC credentials successfully.

To change the request timeout on the controller, follow these steps:

Procedure

-
- Step 1** Use SSH or Telnet to access the Cisco Unified wireless LAN controller.
- Step 2** Enter `config advanced eap request-timeout 20`
- Step 3** Enter `save config`
- Step 4** Enter `y` to confirm.
-

Configuring QoS Policies

To ensure that voice traffic receives the highest priority in the WLAN and to place signaling traffic in a higher priority than data traffic, you need to make these changes to QoS policies and device settings.

Access Point Configuration Settings

For detailed information about configuring the Cisco Aironet Access Points, refer to this URL:

<http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo1200/accsspts/b1238ja/1238jasc/index.htm>

On the IOS access points, add the following Classifications to your IOS Access Point QoS policy:

- DSCP Expedited Forwarding—COS Voice <10ms Latency (6)
Apply this policy to your voice VLAN for both incoming and outgoing traffic.
- DSCP Best Effort—COS Best Effort (0)
Apply this policy to your data or native VLAN for both incoming and outgoing traffic.

Under the Advanced tab, set the following:

- QoS Element for Wireless Phones—Enable.
- Dot11e—Enable.
- IGMP Snooping—Enable.
- AVVID Priority Mapping—Yes.
- WiFi Multimedia (WMM) on radio interfaces—Enabled

Controller Settings

For detailed information about configuring QoS policies for the controller, refer to these URLs:

- <http://www.cisco.com/univercd/cc/td/doc/product/wireless/control/index.htm>
- <http://www.cisco.com/univercd/cc/td/doc/product/wireless/control/c44/ccfig40/index.htm>

When using a controller, add the following QoS policies:

- Platinum (voice)—Apply this policy to your voice WLAN SSID/VLAN for both incoming and outgoing traffic.

- Silver (best effort)—Apply this policy to your data WLAN SSID/VLAN for both incoming and outgoing traffic.
- WLAN configuration screen for the voice WLAN SSID/VLAN—For the 7925G Phone Support field, check the AP CAC Limit checkbox to enable QoS Element for Wireless Phones (QBSS).
- General Controller configuration screen—Set Aggressive Load Balancing to Disabled.

Switch Configuration

To implement QoS in the connected Ethernet switch individual configurations will vary; however, you can use this example of QoS commands as a guide.

```
mls qos
mls qos map cos-dscp 0 8 16 24 34 46 48 56
mls qos map ip-prec-dscp 0 8 16 24 34 46 48 56

interface FastEthernet0/00
switchport access vlan 11
switchport mode access
switchport voice vlan 111
no ip address
mls qos trust dscp
wrr-queue cos-map 1 1
wrr-queue cos-map 2
wrr-queue cos-map 3 2 3 4 6 7
wrr-queue cos-map 4 5
priority queue out
spanning-tree portfast
```



Note

When you are using U-APSD for power save, you must implement proper QoS policies on the access points and Ethernet switch.

Configuring the Cisco Unified Wireless IP Phone 7925G in Cisco Unified Communications Manager

[Table D-2](#) provides an overview and checklist of configuration tasks for the Cisco Unified Wireless IP Phone 7925G 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 D-2 Checklist for Configuring the Cisco Unified Wireless IP Phone 7925G in Cisco Unified CallManager

Configuration Step and Purpose	For More Information
<p>Step 1</p> <p>Gather the following information about the phone:</p> <ul style="list-style-type: none"> • Phone Model • MAC address • Name or user ID of phone user • Device pool • Partition, calling search space, and location information • Number of lines and associated directory numbers (DNs) to assign to the phone • Cisco Unified Communications Manager user to associate with the phone • Phone usage information that affects softkey template, phone features, IP Phone services, or phone applications <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 Telephony Features Available for the Phone, page 7-2.</p>
<p>Step 2</p> <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 CallManager Administration Guide</i>, “Phone Button Template Configuration” chapter.</p> <p>See Modifying Phone Button Templates, page 7-17.</p>
<p>Step 3</p> <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 CallManager 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>
<p>Step 4</p> <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 <i>Cisco Unified Communications Manager Administration Guide</i>:</p> <ul style="list-style-type: none"> • “Directory Number Configuration” chapter • “Creating a Cisco Unity Voice Mailbox” section. <p>See Telephony Features Available for the Phone, page 7-2.</p>
<p>Step 5</p> <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 CallManager Administration Guide</i>, “Softkey Template Configuration” chapter.</p> <p>See Configuring Softkey Templates, page 7-16.</p>

Table D-2 Checklist for Configuring the Cisco Unified Wireless IP Phone 7925G in Cisco Unified CallManager

Configuration Step and Purpose	For More Information
<p>Step 6 Assign line view speed-dial numbers (optional). Adds line view speed-dial numbers.</p> <p>Note Configuring and using line view speed-dial numbers are different from speed-dial hot keys that are set up using the Phone Book feature and stored locally on the wireless IP phone.</p> <p>Note Users can change line view speed-dial settings on their phones by using Cisco Unified CM User Options.</p>	<p>Refer to <i>Cisco Unified CallManager Administration Guide</i>, “Cisco Unified IP Phone Configuration” chapter, “Configuring Speed-Dial Buttons” section.</p> <p>Refer to <i>Cisco Unified Wireless IP Phone 7925G Administration Guide for Cisco Unified Communications Manager 4.3, 5.1, 6.0, 6.1(1) and 7.0(1)</i>, “Advanced Call Handling” chapter, “Speed Dialing” section.</p> <p>See Telephony Features Available for the Phone, page 7-2</p>
<p>Step 7 Configure Cisco Unified IP Phone services and assign services (optional). Provides IP Phone services.</p> <p>Note Users can add or change services on their phones by using the Cisco Unified CM User Options.</p>	<p>Refer to <i>Cisco Unified CallManager Administration Guide</i>, “Cisco Unified IP Phone Services Configuration” chapter.</p> <p>See Setting Up Services, page 7-17.</p>
<p>Step 8 Add user information by configuring required fields. Required fields are indicated by an asterisk (*); for example, User ID and last name.</p> <p>Note Assign a password (for User Options web pages) 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 CallManager Administration Guide</i>, “End User Configuration” chapter.</p> <p>See Adding Users to Cisco Unified Communications Manager, page 7-19.</p>
<p>Step 9 Associate a user to a user group. Assigns users a common list of roles and permissions that apply to all users in a user group. Administrators can manage user groups, roles, and permissions to control the level of access (and, therefore, the level of security) for system users.</p> <p>Note Applicable to Cisco Unified Communications Manager Administration Release 5.x and later.</p>	<p>Refer to the <i>Cisco Unified Communications Manager Administration Guide</i>:</p> <ul style="list-style-type: none"> • “End User Configuration” chapter, “End User Configuration settings” section • “User Group Configuration” chapter, “Adding Users to a User Group” section
<p>Step 10 Associate a user with a phone. This step is optional if you do not want users to have access to User Options. Provides users with control over their phone such as forwarding calls or adding line view speed-dial numbers or services.</p> <p>Note Some phones, such as those used by multiple users, do not have an associated user.</p>	<p>Refer to <i>Cisco Unified CallManager Administration Guide</i>, “End User Configuration” chapter, “Associating Devices to a User” section.</p>

Installing the Cisco Unified Wireless IP Phone 7925G

Table D-3 provides an overview and checklist of installation tasks for the Cisco Unified Wireless IP Phone 7925G. 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 D-3 Checklist for Installing the Cisco Unified Wireless IP Phone 7925G

Task	For More Information
1. Assemble the phone components and charge the battery.	See Installing the Cisco Unified Wireless IP Phone 7925G, page 1-15 .
2. Configure the network profile by using the USB cable and the Cisco Unified Wireless IP Phone 7925G web page.	See Accessing the Web Page for a Phone, page 9-1 .
3. Configure the phone settings by using the Settings menu on the phone.	See Changing Phone Settings, page 5-10 .
4. Power on the phone and monitor the phone startup process.	See Understanding the Phone Startup Process, page 3-17 . See Resolving Startup and Connectivity Problems, page 10-1
5. Make calls with the wireless IP phone.	Refer to the <i>Cisco Unified Wireless IP Phone 7925G Guide</i> . See Resolving Voice Quality and Roaming, page 10-8
6. Provide information to end users about how to use their phones and how to configure their phone options.	See Appendix A, "Providing Information to Users By Using a Website."



INDEX

Numerics

- 802.11a standard [2-3](#)
- 802.11b standard [2-3](#)
- 802.11g standard [2-3](#)

A

- active mode [3-16](#)
- AES
 - encryption description [2-18](#)
- AP
 - associating [2-12](#)
 - Cisco Aironet Access Point [2-11](#)
 - Cisco IOS version for wireless voice [2-21](#)
 - description [2-11](#)
 - troubleshooting [10-2](#)
- AP settings, identifying [10-8](#)
- audience, for this document [1-xi](#)
- authenticated call [1-12](#)
- authentication [5-12](#)
 - selecting type [5-9](#)
 - wireless network setting [5-9](#)
- auto-pickup [7-2](#)
- auto-registration
 - using [3-3](#)
 - using with TAPS [3-3](#)
- auxiliary VLAN, description [2-12](#)

B

- barge [1-13, 7-3](#)
- BAT (Bulk Administration Tool) [3-4](#)

- battery
 - charging times with power supply [3-8](#)
 - description [3-7](#)
 - installing and removing [3-7](#)
 - types available [3-7](#)
- battery caution [3-6](#)
 - charging [3-7](#)
 - damaged [3-6](#)
 - disposal [3-7](#)
 - replacement re [3-7](#)
 - temperature [3-7](#)
- battery safety notices [3-6](#)
- battery warning
 - disposal [3-6](#)
 - explosion [3-6](#)
- block external to external transfer [7-3](#)
- Bluetooth qualified device [1-2, 2-8](#)
- Bluetooth technology
 - adaptive frequency hopping [1-2](#)
 - headset pairing [1-3](#)
 - overview [1-2](#)
 - pairing headsets [3-14](#)
 - power and range by class [1-2](#)
 - unlicensed band [1-2](#)
 - using Bluetooth wireless headsets [3-14](#)
- Busy Lamp Field (BLF) speed dial [7-3](#)

C

- call
 - authenticated [1-12](#)
 - encrypted [1-12](#)
 - protected [1-13](#)

- Call Back [7-3](#)
 - call display restrictions [7-4](#)
 - caller ID [7-5](#)
 - call forward
 - all calls [7-4](#)
 - display, configuring [7-4](#)
 - loop breakout [7-4](#)
 - loop prevention [7-4](#)
 - call forward display, configuring [7-4, 7-6](#)
 - call park [7-5](#)
 - call pickup [7-5](#)
 - call statistics screen [8-1, 8-14](#)
 - call waiting [7-5](#)
 - CAPF (Certificate Authority Proxy Function) [1-11, 5-12](#)
 - cautions
 - for battery pack [3-6](#)
 - for charging battery pack [3-7](#)
 - for damaged battery [3-6](#)
 - for disposing of battery pack [3-7](#)
 - for exposing battery pack to high temperatures [3-7](#)
 - for replacing battery pack [3-7](#)
 - for replacing power supply [3-7](#)
 - translations [3-5](#)
 - CDP
 - description [2-10](#)
 - CDP settings [5-7](#)
 - change password web page [4-38](#)
 - Cisco Discovery Protocol, See CDP
 - Cisco IOS version, supporting wireless voice LAN [2-21](#)
 - Cisco Unified Communications Manager
 - adding phone to database of [3-2](#)
 - configuring DHCP settings [2-15](#)
 - interacting with [2-14](#)
 - restricting phone settings access [5-1, 5-2, 5-10](#)
 - verifying settings [10-5](#)
 - Cisco Unified Communications Manager Administration
 - adding telephony features [7-2](#)
 - Cisco Unified IP Phone
 - configuration requirements [D-1](#)
 - installation overview [D-1](#)
 - installation requirements [D-1](#)
 - online help for [A-3](#)
 - using LDAP directories [7-19](#)
 - Cisco Unified Wireless IP Phone
 - overview [1-1](#)
 - web page [4-1, 9-1](#)
 - Cisco Unified Wireless IP Phone, See also wireless IP phone
 - Cisco Unified Wireless IP Phone specifications [C-1](#)
 - client matter codes [7-6](#)
 - conference [7-6](#)
 - configurable call forward display [7-6](#)
 - configuration file
 - creating new [10-7](#)
 - encrypted [1-11](#)
 - overview [2-14](#)
 - SEPxxxxxxxxxxxxx.cnf.xml [2-14](#)
 - XMLDefault.cnf.xml [2-14](#)
 - configuring
 - AP tasks [D-1](#)
 - LDAP directories [7-19](#)
 - overview [D-1](#)
 - personal directories [7-19](#)
 - phone book [4-29](#)
 - softkey templates [7-16](#)
 - user features [7-19](#)
 - Wavelink settings [4-29, 6-1](#)
 - CTL file
 - unlocking [8-3](#)
 - CTL file screen [8-3](#)
 - current configuration
 - viewing [8-9, 8-12](#)
-
- D**
- data VLAN [2-12](#)
 - device authentication [1-10](#)
 - device information menu, about [8-1](#)

device information web page [9-6](#)

DHCP

description [2-10](#)

displaying settings [5-6](#)

enable, network setting [5-4](#)

gateway [2-15](#)

interacting with [2-15](#)

IP address [2-15](#)

modifying settings [5-6](#)

priority for TFTP server [2-15](#)

scope settings [2-15](#)

subnet mask [2-15](#)

troubleshooting [10-9](#)

directed call park [7-7](#)

directory numbers, assigning manually [3-4](#)

direct-sequence spread spectrum (DSSS) [2-5](#)

direct transfer [7-7](#)

displaying, network statistics [8-12](#)

disposal warning [3-6](#)

DNS server

settings for TFTP server [2-15](#)

troubleshooting [10-9](#)

verifying settings [10-5](#)

documentation

additional [1-xiii](#)

for users [A-3](#)

localized versions [B-1](#)

dynamic host configuration protocol, See DHCP

E

editing configuration values, guidelines [5-4](#)

encrypted call [1-12](#)

encrypted configuration file [1-11](#)

encryption

media [1-11](#)

signaling [1-11](#)

WEP key [4-16](#)

erase configuration, procedure [10-18](#)

explosive gas warning [3-5](#)

extension mobility, description [7-8](#)

F

features

configuring with Cisco Unified Communications Manager [1-7](#)

See also telephony features

file

creating new configuration [10-7](#)

file authentication [1-10](#)

firmware

verifying version [8-16](#)

forced authorization codes [7-9](#)

G

group call pickup [7-9](#)

H

help, using [A-3](#)

hold [7-9](#)

hold reversion [7-9](#)

hunt group [7-9](#)

I

icon

lock [1-12](#)

padlock [1-12](#)

shield [1-12](#)

image authentication [1-10](#)

immediate divert [7-9](#)

Immediate Divert enhanced feature [7-10](#)

installation

AP configuration tasks [D-1](#)

network requirements [3-1](#)

preparing [3-2](#)
 installation warning [3-5](#)
 installing
 requirements, overview [D-1](#)
 intercom [7-10](#)
 International Call Logging [B-2](#)
 Internet Protocol (IP) [2-10](#)
 IP, description [2-10](#)
 IP address [2-15, 4-24, 5-6](#)
 troubleshooting [10-5](#)

J

join [7-10](#)
 join across lines [7-10](#)

L

LDAP directories, using with Cisco Unified IP
 Phone [7-19](#)
 LEAP
 description [2-17](#)
 light extensible authentication protocol, See LEAP
 local configuration, erasing [10-18](#)
 Locale Installer [B-1](#)
 localization
 Installing the Cisco Unified Communications Manager
 Locale Installer [B-1](#)
 Locally Significant Certificate (LSC) [5-12](#)
 lock icon [1-12](#)

M

MAC address
 determining [3-2](#)
 malicious caller identification (MCID) [7-10](#)
 manufacturing installed certificate (MIC) [1-11](#)
 media encryption [1-11](#)
 meet-me conference [7-10](#)

message waiting [7-11](#)
 metrics, voice quality [8-15, 9-11](#)
 MIC [1-11](#)
 model information screen [8-1](#)
 music-on-hold [7-11](#)

N

native VLAN [2-12](#)
 neighbor list utility [2-23](#)
 network configuration menu
 displaying [5-3](#)
 displaying WLAN configuration menu [5-8](#)
 editing options [5-4](#)
 network configuration web page [9-2, 9-3](#)
 network connectivity, verifying [10-4](#)
 networking protocol
 CDP [2-10](#)
 DHCP [2-10](#)
 IP [2-10](#)
 RTP [2-10](#)
 SCCP [2-10](#)
 supported [2-9](#)
 TCP [2-11](#)
 TFTP [2-11](#)
 TLS [2-11](#)
 UDP [2-11](#)
 network outages, identifying [10-8](#)
 network protocol
 LEAP [2-17](#)
 RTCP [2-10](#)
 network requirements, for installation [3-1](#)
 network settings
 accessing on phone [5-1](#)
 configuring [5-1](#)
 DHCP enable [5-4](#)
 network statistics [9-9](#)
 network statistics, viewing [8-12](#)
 network statistics web page [9-2](#)

O

- on hook call transfer [7-11](#)
- online help, using [A-3](#)
- open authentication, description [2-16](#)
- orthogonal frequency division multiplexing (OFDM) [2-3, 2-6](#)
- other group pickup [7-11](#)

P

- padlock icon [1-12](#)
- personal directories, configuring [7-19](#)
- phone book, using [4-29](#)
- phone mode
 - active [3-16](#)
 - standby [3-17](#)
- phone operation for users [A-1](#)
- phone resets, resolving problems [10-8](#)
- phones, installing [1-15](#)
- phone settings
 - access restrictions [5-1, 5-2, 5-10](#)
 - menu [5-11](#)
- phone upgrade web page [4-37](#)
- phone web page
 - about [4-1, 9-1](#)
 - accessing [4-5, 9-1](#)
 - change password [4-38](#)
 - device information [9-6](#)
 - installing drivers [4-1](#)
 - network configuration [9-3](#)
 - network statistics [9-2, 9-9](#)
 - phone upgrade [4-37](#)
 - profile settings [4-8](#)
 - summary information [4-7, 9-2](#)
 - system settings [4-34](#)
 - trace logs [4-34](#)
 - trace settings [4-27](#)
 - USB settings [4-26](#)

- plug-socket warning [3-5](#)
- powering on phone [3-15](#)
- power outage warning [3-5](#)
- power supply
 - figure, connected [3-11](#)
- power supply replacement caution [3-7](#)
- power supply warning [3-6](#)
- presence-enabled directories [7-11](#)
- primary DNS server [2-16, 4-24, 5-7](#)
- primary gateway [2-15, 4-24, 5-6](#)
- primary TFTP server [5-7](#)
- privacy [7-11](#)
- profile settings web page [4-8](#)
- protected call [1-13](#)
 - description [1-13](#)
- Protected Calls [1-13](#)
- Push to Talk service [7-11](#)

Q

- QBSS, description [2-12](#)
- QDID [1-2, 2-8](#)
- QoS basis service set, See QBSS
- QRT softkey [7-12](#)
- Quality of Service (QoS) [2-12](#)
- Quality Reporting Tool (QRT) [7-12](#)

R

- RADIUS server authentication, description [2-17, 2-18](#)
- real-time control protocol, See RTCP
- real-time transport protocol, See RTP
- received signal strength indicator, See RSSI
- redial [7-12](#)
- resetting, phones [10-9](#)
- resolving startup problems [10-1 to 10-7](#)
- resolving voice quality problems [10-8 to 10-12](#)
- ring activity [7-12](#)
- ringlist.xml [7-21](#)

ring tone, creating custom [7-21](#)

roaming [2-7](#)

fast and secure with CCKM [2-7](#)

layer 3 [2-7](#)

Layer 3 with WLSM [2-7](#)

mid-call [2-7](#)

pre-call [2-7](#)

resolving problems [10-8](#)

RSSI, description [2-12](#)

RTCP, description [2-10](#)

RTP description [2-10](#)

S

SCCP description [2-10](#)

secure SRST reference [1-11](#)

security

AES encryption [2-18](#)

CAPF (Certificate Authority Proxy Function) [1-11](#),
[5-12](#)

device authentication [1-10](#)

encrypted configuration file [1-11](#)

file authentication [1-10](#)

image authentication [1-10](#)

manufacturing installed certificate (MIC) [1-11](#)

media encryption [1-11](#)

open authentication [2-16](#)

RADIUS server authentication [2-17](#), [2-18](#)

secure SRST reference [1-11](#)

security profiles [1-11](#), [1-12](#)

shared key authentication [2-16](#)

signaling authentication [1-10](#)

signaling encryption [1-11](#)

static WEP encryption [2-18](#)

TKIP encryption [2-18](#)

WLAN overview [2-16](#)

WPA authentication [2-18](#)

WPA-Pre-shared key authentication [2-16](#)

security configuration menu, about [8-1](#)

security profiles [1-11](#), [1-12](#)

SEPxxxxxxxxxxxx.cnf.xml configuration file [2-14](#)

services

description [7-12](#)

subscribing to [7-17](#)

service set identifier, See SSID

shared key authentication, description [2-16](#)

shared lines [7-12](#)

shield icon [1-12](#)

short circuit protection warning [3-6](#)

signaling authentication [1-10](#)

signaling encryption [1-11](#)

site survey

performing [2-22](#)

verification steps [2-23](#)

site survey utility

display values [2-23](#)

skinny client control protocol, See SCCP

softkey templates, configuring [7-16](#)

specifications

operating environment [C-1](#)

physical [C-1](#)

speed dial

default buttons for [7-17](#)

hot key, assigning [4-33](#)

speed dialing [7-2](#), [7-12](#)

SRST [9-5](#)

secure reference [1-11](#)

SSID

description [5-9](#)

wireless network setting [5-9](#)

standby mode [3-17](#)

startup

resolving problems with [10-1](#)

startup process

contacting Cisco Unified Communications
Manager [3-19](#)

DHCP disabled [2-15](#)

static settings

- IP address [2-15, 4-24, 5-6](#)
 - primary DNS server [2-16, 4-24, 5-7](#)
 - primary gateway [2-15, 4-24, 5-6](#)
 - primary TFTP server [5-7](#)
 - subnet mask [2-15, 4-24, 5-6](#)
 - statistics
 - call [8-14](#)
 - network [9-9](#)
 - statistics, network [8-12](#)
 - status information [8-9, 8-12](#)
 - status menu [8-1, 8-8](#)
 - subnet mask [2-15, 4-24, 5-6](#)
 - summary information web page [4-7](#)
 - survivable remote site telephony (SRST)
 - IP address of router [8-4](#)
 - symptom
 - phone resets [10-8](#)
 - system log server [10-18](#)
-
- T**
- TAPS (Tool for Auto-Registered Phones Support) [3-3](#)
 - TCP
 - description [2-11](#)
 - telephone receiver warning [3-6](#)
 - telephony features
 - auto-pickup [7-2](#)
 - barge [1-13, 7-3](#)
 - block external to external transfer [7-3](#)
 - Busy Lamp Field (BLF) speed dial [7-3](#)
 - call display restrictions [7-4](#)
 - caller ID [7-5](#)
 - call forward [7-4](#)
 - call forward configurable display [7-4](#)
 - call park [7-5](#)
 - call pickup [7-5](#)
 - call waiting [7-5](#)
 - Cisco Call Back [7-3](#)
 - client matter codes [7-6](#)
 - conference [7-6](#)
 - configurable call forward display [7-6](#)
 - configuration references [7-2](#)
 - descriptions [7-2](#)
 - directed call park [7-7](#)
 - direct transfer [7-7](#)
 - extension mobility [7-8](#)
 - forced authorization codes [7-9](#)
 - group call pickup [7-9](#)
 - hold [7-9](#)
 - hold reversion [7-9](#)
 - hunt group [7-9](#)
 - immediate divert [7-9](#)
 - join [7-10](#)
 - malicious caller identification (MCID) [7-10](#)
 - meet-me conference [7-10](#)
 - music-on-hold [7-11](#)
 - no not disturb (DND) [7-8](#)
 - on hook call transfer [7-11](#)
 - other group pickup [7-11](#)
 - presence-enabled directories [7-11](#)
 - Push to Talk service (XML application) [7-11](#)
 - redial [7-12](#)
 - ring activity [7-12](#)
 - services [7-12](#)
 - shared lines [7-12](#)
 - speed dialing [7-12](#)
 - supported [7-2](#)
 - Time-of-Day Routing [7-13](#)
 - transfer [7-13](#)
 - voice messaging system [7-13](#)
 - template
 - phone button, modifying [7-17](#)
 - TFTP
 - description [2-11](#)
 - troubleshooting [10-4](#)
 - TFTP server
 - assigning to phone [4-24, 5-7](#)
 - options [4-24, 5-7](#)

Time-of-Day Routing [7-13](#)

TKIP

- encryption description [2-18](#)

trace logs web page [4-34](#)

trace route

- option on phone [10-18](#)

trace settings web page [4-27](#)

transfer [7-13](#)

transmission control protocol, See TCP

transport layer security

- See TLS

trivial file transfer protocol, See TFTP

troubleshooting

- AP settings [10-2, 10-8](#)
- Cisco Unified Communications Manager settings [10-5](#)
- DHCP [10-9](#)
- DNS [10-9](#)
- DNS settings [10-5](#)
- general information [10-14](#)
- IP addressing and routing [10-5](#)
- logging information [10-17](#)
- network connectivity [10-4](#)
- network outages [10-8](#)
- phones resetting [10-9](#)
- services on Cisco Unified Communications Manager [10-6](#)
- TFTP settings [10-4](#)
- VLAN configuration [10-9](#)
- wireless IP phone [10-1](#)

Trust List screen [8-4](#)

U

UDP description [2-11](#)

USB configuration [4-1](#)

- displaying menu [5-13](#)

USB settings web page [4-26](#)

user datagram protocol, See UDP

User Options web page

- description [7-20](#)
- giving users access to [7-20](#)
- specifying options that appear [7-21](#)

users

- accessing voice messages [A-4](#)
- documentation for [A-3](#)
- international, supporting [B-1](#)
- required information [A-1](#)
- wireless IP phone information [A-1](#)

V

verifying

- Cisco Unified Communications Manager settings [10-5](#)
- firmware version [8-16](#)
- network settings [10-4](#)

VLAN

- assigning separate SSIDs [2-12](#)
- auxiliary, for voice traffic [2-12](#)
- native, for data traffic [2-12](#)
- separate voice for QoS [2-12](#)
- verifying [10-9](#)

voice messaging system [7-13](#)

voice quality, resolving problems [10-8](#)

voice quality metrics [8-15, 9-11](#)

voice VLAN [2-12](#)

W

warnings

- definition [3-5](#)
- for battery disposal [3-6](#)
- for battery explosion [3-6](#)
- for disposal [3-6](#)
- for explosive gas [3-5](#)
- for installation [3-5](#)
- for plug socket [3-5](#)

- for power outages [3-5](#)
 - for power supply [3-6](#)
 - for short circuit protection [3-6](#)
 - for telephone receiver [3-6](#)
 - translations [3-5](#)
 - Wavelink software, using [4-29, 6-1](#)
 - WDS, wireless domain server [2-8](#)
 - web page
 - configuring phone settings [4-1](#)
 - WEP encryption, description [2-18](#)
 - WEP key
 - setting up encryption [4-16](#)
 - Wi-Fi (802.11b) [2-3](#)
 - wireless domain server (WDS) [2-8](#)
 - wireless IP phone
 - adding manually to Cisco Unified Communications Manager [3-4](#)
 - adding to Cisco Unified Communications Manager [3-2](#)
 - adding using auto-registration [3-3](#)
 - adding using auto-registration with TAPS [3-3](#)
 - adding using BAT [3-4](#)
 - battery [3-7](#)
 - configuration file [2-14](#)
 - feature overview [1-6](#)
 - figure [1-4](#)
 - keys [1-4](#)
 - phone modes, active and standby [3-16](#)
 - powering on [3-15](#)
 - registering [3-2](#)
 - registering with Cisco Unified Communications Manager [3-3, 3-4](#)
 - supported networking protocols [2-9](#)
 - troubleshooting [10-1](#)
 - troubleshooting tips [10-14](#)
 - wireless IP phone, See also Cisco Unified Wireless IP Phone
 - wireless local area network, See WLAN
 - wireless network settings
 - authentication [5-9](#)
 - SSID [5-9](#)
 - WLAN
 - components [2-9](#)
 - security [2-16](#)
 - voice quality [2-12](#)
 - WLAN configuration menu [5-8](#)
 - WLSM, wireless LAN services module [2-7](#)
 - WPA
 - encryption with TKIP, description [2-18](#)
 - WPA authentication, description [2-18](#)
 - WPA-pre-shared key authentication, description [2-16](#)
-
- X**
- XMLDefault.cnf.xml configuration file [2-14](#)

