Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G Administration Guide

First Published: April 08, 2012

Last Modified: August 09, 2013

CONTENTS

Preface

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

Overview

Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G Administration Guide provides the information you need to understand, install, configure, and manage the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G on your network. This guide is intended to be used to administer phones running with Cisco Unified Communications Manager Release 4.3 and later.

Audience

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

Organization

This guide is organized as follows:

Related documentation

Use the following sections to obtain related information.

Cisco Unified IP Phone 7900 Series documentation

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

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

Cisco Unified Communications Manager documentation

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

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

Cisco Business Edition 5000 documentation

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

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

Documentation, support, and security guidelines

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

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.

Guide conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[ ]	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 screen font.
input font	Information you must enter is in input font.
italic screen font	Arguments for which you supply values are in *italic screen* font.
^	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.

Warnings use the following convention:

⚠

Attention   IMPORTANT SAFETY INSTRUCTIONS

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

SAVE THESE INSTRUCTIONS

Cisco Unified Wireless IP Phone

The Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G provides wireless voice communication over an IP network. As with 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.

For information about the phones and accessories, see the following documents:

- *Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G User Guide*
- *Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G Accessory Guide*

This chapter includes the following sections:

Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G

This section describes the phone components.

Cisco Unified Wireless IP Phone 7925G and 7926G

The Cisco Unified Wireless IP Phone 7925G and 7926G are 802.11 dual-band wireless devices that provide comprehensive voice communications in conjunction with Cisco Unified Communications Manager and with Cisco Aironet 802.11b/g and Cisco Aironet 802.11a access points (APs) in a private business communications network.

The phone is a qualified Bluetooth wireless device (Qualified Device ID [QDID] B014396). The phone provides voice communication over the same wireless LAN that your computer uses, allowing you to place and receive phone calls, put calls on hold, transfer calls, make conference calls, and so on.

The following figure shows the Cisco Unified Wireless IP Phone 7925G. The Cisco Unified Wireless IP Phone 7926G looks similar.

This phone model, like other network devices, must be configured and managed. This phone encodes G.711a, G.711u, G.729a, G.729ab, and G.722/iLBC codecs, and decodes G.711a, G711b, G.711u, G.729, G729a, G729b, and G729ab codecs. The phone also supports uncompressed wideband (16 bits, 16 kHz) audio.

The Cisco Unified Wireless IP Phone 7925G and 7926G is hearing aid compatible (HAC) but do not have any TTY features. They have 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 antibacterial and alcohol-based wipes
- Latex- and lead-free
- Resistance against liquid splashes
- Dust resistance
- Shockproof and vibration-proof
- USB 1.1 interface

In addition to basic call-handling features, your phone can provide enhanced productivity features that extend your call-handling capabilities.

Depending on the configuration, your phone supports:

- Use of Bluetooth wireless headsets, including certain hands-free call features
- Wireless access to your phone number and the corporate directory
- A local phone book that can store up to 200 contacts and speed-dial hot keys that can be assigned to phone book contacts

- Access to network data, XML applications, and web-based services

- Online customizing of phone features and services from your User Options web pages

- An online help system that displays information on the phone screen

The Cisco Unified Wireless IP Phone 7926G contains a bar code scanner.

Cisco Unified Wireless IP Phone 7925G-EX

Your Cisco Unified Wireless IP Phone 7925G-EX is an Atmospheres Explosibles (ATEX) Zone 2/Class 22 and Canadian Standards Association (CSA) Division 2/Class 1 certified full-feature telephone. The phone is certified for use in potentially explosive environments in the gas, oil, and chemical production fields as well as dust-filled environments. The phone has Ingress Protection 64 (IP 64) level protection, indicating dust-tight equipment that is protected against splashing water. The phone has an industry-standard yellow styling that offers fast recognition in emergency situations.

The phone is a qualified Bluetooth wireless device (Qualified Device ID [QDID] B014396). The phone provides voice communication over the same wireless LAN that your computer uses, allowing you to place and receive phone calls, put calls on hold, transfer calls, make conference calls, and so on.

The following figure shows the Cisco Unified Wireless IP Phone 7925G-EX.

This phone model, like other network devices, must be configured and managed. This phone encodes G.711a, G.711u, G.729a, G.729ab, and G.722/iLBC codecs, and decodes G.711a, G711b, G.711u, G.729, G729a, G729b, and G729ab codecs. The phone also supports uncompressed wideband (16 bits, 16 kHz) audio.

The Cisco Unified Wireless IP Phone 7925G-EX 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:

- Atmospheres Explosibles (ATEX) Zone 2/Class 22 certification prevents ignition of surrounding gas vapors by the phone.

- Canadian Standards Association (CSA) Division 2/Class 1 certification provides access to mobile collaborative communications.

- Industry-standard yellow styling offers fast recognition in emergency situations.

- Ingress Protection 64 (IP 64) level protection, indicating dust-tight equipment which is protected against splashing water.

- The large 2-inch color (176 x 220 pixels) display makes viewing easy.

- Resistance to damage from dropping the phone.

- Tolerance of antibacterial and alcohol-based wipes.

- Latex- and lead-free.

- Shockproof and vibration-proof.

- USB 1.1 interface.

Note   ATEX Zone 2 certification: Zone 2 is defined as an area in which an explosive gas atmosphere is not likely to occur in normal operation and if it does occur, is likely to do so only infrequently and will exist for a short period only (for example, less than 10 hours per year).

Note   CSA Class 1 Division II certification: Class 1 is a location where a quantity of flammable gas or vapor sufficient to produce an explosive or ignitable mixture may be present in the air. Division II is a location where a classified hazard does not normally exist but is possible under abnormal conditions.

In addition to basic call-handling features, your phone can provide enhanced productivity features that extend your call-handling capabilities.

Depending on the configuration, your phone supports:

- Use of Bluetooth wireless headsets, including certain hands-free call features

- Wireless access to your phone number and the corporate directory

- A local phone book that can store up to 200 contacts and speed-dial hot keys that can be assigned to phone book contacts

- Access to network data, XML applications, and web-based services

- Online customizing of phone features and services from your User Options web pages

Buttons and Hardware

The following figure shows the Cisco Unified Wireless IP Phone 7926G. The Cisco Unified Wireless IP Phone 7925G and 7925G-EX are similar in appearance to the Cisco Unified Wireless IP Phone 7926G. The following table describes the functions of the keys on the phones.

1	Indicator light (LED)	Provides these indications:
		• 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: There is an incoming call. Phone can be charging or fully charged.
		• Slow blinking red: There is a voice message. When phone is connected to AC power source, the red light displays longer than when using only the battery.
		• Slow blinking green (every 2 seconds): Phone is using only battery power. Phone is registered with the wireless network and is within service coverage area.
2	Headset port with cover	Port for plugging in a headset or ear bud has a protective cover.
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	Accesses these menus and lists from the main screen:
		Directory
		Line View
		Settings
		Services
		Allows you to scroll up and down menus to highlight options and to move left and right through phone numbers and text entries.
6	Select button	Activates the Help menu from the main screen.
		Allows you to select a menu item, a softkey, a call, or an action.
7	Power/End button (red)	Turns the phone on or off, ends a connected call, or silences the ring during an incoming call.
		When you use menus, acts as a shortcut to return to the main screen.
8	Pound (#) key	Allows you to lock the keypad.
		Allows you to enter these special characters when you are entering text: **# ? ( ) [ ] { }**
9	Zero (0) key	Enters "0" when you dial a number. Allows you to enter a space or these special characters when you are entering text: **, . ' " | _ ~ '**
10	Asterisk (*) key	Toggles between ring and vibrate mode.
		Allows you to enter these special characters when you are entering text: *** + - / = \ : ;**
11	Keypad	Allows you to dial numbers, enter letters, and choose menu items by number.
12	One (1) key	Enters "1" when you dial a number. Allows you to access voice mail.
		Allows you to enter these special characters when you are entering text: **! @ < > $ % ^ &**
13	Answer/Send button (green)	Allows you to answer a ringing call or, after dialing a number, to place the call.
14	Left softkey button	Activates the softkey option displayed on the screen.

		When you set it up, allows you to directly access your messages or open the Phone Book when the phone is idle.
15	Mute button	Toggles the mute feature on or off.
16	Volume button	When the phone is idle, allows you to control the ring volume, turn on the vibrate option, or turn off the ring.
		When an incoming call is ringing, allows you to press this button once to silence the ring for the call.
		During a call, allows you to control the speaker volume for the handset, headset, and speaker mode.
		When the phone is docked in the desktop charger, the volume button on the phone controls the volume of the charger speaker.
17	Application button	Use with XML applications, such as Push to Talk or other services.
18	Bar code scanner	Use with Java MIDlet applications to allow you to scan bar codes.
		Note Available only on the Cisco Unified Wireless IP Phone 7926G.

Cisco Unified Wireless IP Phone 7925G Desktop Charger Overview

The Cisco Unified Wireless IP Phone 7925G Desktop Charger provides the following features:

- Charges the docked phone battery from line power
- Contains a speakerphone, with the volume controlled by the phone volume buttons
- Supports Bluetooth through the speakerphone
- Displays status information using the Power/Bluetooth Status LED and Battery LED
- Contains an additional port at the back of the station for charging a spare battery
- Works on line power or from the spare battery for the phone

The following figure shows the Cisco Unified Wireless IP Phone 7925G docked in the Cisco Unified Wireless IP Phone 7925G Desktop Charger.

Figure 1: Cisco Unified Wireless IP Phone 7925G docked in the charger

The Cisco Unified Wireless IP Phone 7925G Desktop Charger supports the following phones:

- Cisco Unified Wireless IP Phone 7925G

- Cisco Unified Wireless IP Phone 7925G-EX

- Cisco Unified Wireless IP Phone 7926G

The two LEDs on the Cisco Unified Wireless IP Phone 7925G Desktop Charger change color, as described in the following table.

LED	Color	Flash rate	Meaning
Power/Bluetooth Status	Unlit	Solid	The charger is not plugged into line power.
	Green	Solid	The charger is plugged into line power.
	Blue	Flashing slowly	Bluetooth is connecting or disconnecting from the charger.
		Solid	The charger is connected to the phone using Bluetooth.
Battery	Unlit	Solid	No spare battery is installed.
	Red	Solid	The spare battery is charging.
	Green	Solid	The spare battery is fully charged.
	Amber-yellow	Solid	The station is powered by the spare battery with adequate charge.
		Flashing	The station is powered by the spare battery, but the battery is low.
		Flashing and dimming slowly	The station is powered by the spare battery, but the battery is rapidly depleting.

The spare battery charges only when the Cisco Unified Wireless IP Phone 7925G Desktop Charger is plugged into line power.

The Cisco Unified Wireless IP Phone 7925G Desktop Charger supports Bluetooth Version 2.1 + Extended Data Rate (EDR) using Hands-free Version 1.5.

The following figure shows the location of the Control button. The Control button is used when pairing the charger with the phone.

Control
button

Bluetooth technology

The Cisco Unified Wireless IP Phones are full-feature telephones and a qualified Bluetooth wireless devices (Qualified Device ID [QDID] B014396) and provide voice communication over the same wireless LAN that your computer uses. In addition to basic call-handling features, your phone operates with Bluetooth wireless headsets, including certain hands-free call features.

Bluetooth devices operate in the unlicensed Industrial Scientific Medicine (ISM) band of 2.4 GHz, which is the same as the 802.11b/g band. This unlicensed band in most countries includes the frequency range from 2400 to 2483.5 MHz. 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 uses integrated Adaptive Frequency Hopping (AFH) to avoid interference. Every 625 microseconds (1/1,000,000 of a second) the channel changes or hops to another frequency within the 2402 to 2480 MHz range. This equals 1600 hops every second.

The Cisco Unified Wireless IP Phones contain a Bluetooth module and 802.11 WLAN module. This coexistence greatly reduces and avoids radio interference between the Bluetooth and 802.11b/g radio.

Bluetooth devices fit into to three different power classes, as shown in the following table.

Table 1: Bluetooth maximum permitted transmit power and range by class

Class	Maximum permitted transmit power (mW, dBm)	Range
Class 1	100 mW, 20 dBm	Up to 100 meters

Class	Maximum permitted transmit power (mW, dBm)	Range
Class 2	2.5 mW, 4 dBm	Up to 10 meters
Class 3	1 mW, 0 dBm	Up to 1 meter

Bluetooth Class 2.0 with Extended Data Rate (EDR) is a short-range wireless technology that is supported by the Cisco Unified Wireless IP Phones. The phones support the Hands-Free Profile Version 1.5.

Because of potential interference issues, Cisco recommends 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 on the same side of the body as the Bluetooth-enabled headset.

⚠

Caution Use CSA or ATEX qualified Bluetooth accessories with the Cisco Unified IP Phone 7925G-EX in hazardous environments.

For information about pairing headsets, see Headset usage, on page 62.

For more information about WLAN configuration and Bluetooth, see Site Survey Verification, on page 45. *Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G User Guide* contains user-specific information.

For more information about Bluetooth and hands-free profiles, see http://www.bluetooth.com.

Hands-Free Profile

Your phone supports certain features of the Hands-free 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. 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.

⚠

Caution Use CSA or ATEX qualified bluetooth accessories with the Cisco Unified IP Phone 7925G-EX in hazardous environments.

These hands-free features apply to Bluetooth wireless headsets used with your Cisco Unified Wireless IP Phone:

Redial

Re-calls 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 these 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** Hands-free devices may differ in how features are activated. Hands-free device manufacturers may also use different terms when referring to the same feature.
>
> For more information on using hands-free features, see the documentation provided by the device manufacturer.

Feature Support

The Cisco Unified Wireless IP Phone 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.

Feature Overview

The Cisco Unified Wireless IP Phone provides traditional telephony functionality, such as call forward and call transfer, call pickup, redial, speed dial, conference calls, and voice message 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

- Autodetection of headset and autoanswer 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

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 Telephony features available, on page 150 and *Cisco Unified Communications Manager Administration Guide* for additional information.

For more information about the Cisco Unified Communications Manager Administration, see 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.

Network Settings

As with other network devices, you must configure wireless 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 web pages

- Network Profiles menu on the Cisco Unified Wireless IP Phone

You access the configuration web pages by using a browser from your PC. You configure network settings on the phone itself.

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.

Related Topics

Information for End 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 documentation. Make sure you 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 Wireless IP Phone features (including features specific to your company or network) and about how to access and customize those features, if appropriate.

Related Topics

Internal Support Website, on page 231

Security features

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, see Authentication methods, on page 39.

For information about security features supported by Cisco Unified Communications Manager and Cisco Unified Wireless IP Phones, see Supported security features, on page 15.

The following table provides additional information about security topics.

Table 2: Security topics

Topic	Reference
Detailed explanation of security, including setup, configuration, and troubleshooting information for Cisco Unified Communications Manager and Cisco Unified IP Phones	See *Cisco Unified Communications Manager Security Guide*
Security features supported on the Cisco Unified IP Phone	See Supported security features, on page 15
Restrictions regarding security features	See Security Restrictions, on page 19
Viewing a security profile name when running Cisco Unified Communications Manager 5.0 or later	See Security Profiles, on page 17
Identifying phone calls for which security is implemented	See Authenticated, Encrypted, and Protected Phone Calls, on page 18
Transport Layer Security (TLS) connection	See Network protocols, on page 32 See Phone Configuration Files and Profile Files, on page 37
Security and the phone startup process	See Phone startup process, on page 66
Security and phone configuration files	See Phone Configuration Files and Profile Files, on page 37

Topic	Reference
Changing the TFTP Server 1 or TFTP Server 2 option on the phone when security is implemented	See Network Profiles, on page 76
Items on the Security Configuration menu on the phone	See Display Security Configuration screen, on page 175
Unlocking the CTL file	See CTL File Screen, on page 177
Disabling access to phone web pages	See Product-specific fields for Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G, on page 163
Troubleshooting	See Common Phone Status Messages, on page 223 See *Cisco Unified Communications Manager Security Guide*, Troubleshooting chapter
Resetting or restoring the phone	See Reset phone to factory defaults, on page 228

Supported security features

The following table provides an overview of the security features that the Cisco Unified Wireless IP Phone supports. For more information about these features and about Cisco Unified Communications Manager and Cisco Unified IP Phone security, see *Cisco Unified Communications Manager Security Guide*.

For information about current security settings on a phone, choose **SETTINGS** > **System Configuration** > **Security**. For more information, see Display Security Configuration screen, on page 175.

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

Table 3: Security features description

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.

Feature	Description
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 Set up phone security certificate, on page 132 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.
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 Cisco Unified Survivable Remote Site Telephony (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.

Feature	Description
CAPF (Certificate Authority Proxy Function)	Implements parts of the certificate generation procedure that are too processing-intensive for the phone, and it interacts with the phone for key generation and certificate installation. The CAPF can be configured to request certificates from customer-specified certificate authorities on behalf of the phone, or it can be configured to generate certificates locally.
Security profiles	Defines whether the phone is nonsecure, authenticated, or encrypted. See Security Profiles, on page 17 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: • Disabling Gratuitous ARP (GARP) • Disabling access to the Setting menus • Disabling access to web pages for a phone **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 Display Security Configuration screen, on page 175.

Related Topics

Security Profiles

A security profile defines whether the phone is nonsecure, authenticated, encrypted, or protected. Every Cisco Unified IP Phone that is supported by Cisco Unified Communications Manager Administration has a security profile. For information about configuring the security profile and applying the profile to the phone, see *Cisco Unified Communications Manager Security Guide*.

Note For Cisco Unified Wireless IP Phones using Cisco Unified CallManager 4.3 and later, security is configured on each phone. For more information about configuring security, see *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**.

Related Topics

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 that 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 authenticate using Cisco Unified Communications Manager. When an in-progress call 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 an in-progress call 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, the 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 nonprotected phone, the security tone does not play.

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

Protected Calls Identification

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

The system establishes a protected call 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 the icon 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 nonprotected phone, the secure tone does not play.

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

Related Topics

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 (fast busy) tone plays on the barge initiator phone.

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

If the 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 nonsecure. The authentication icon continues to display on the authenticated phones in the call, even if the initiator's phone does not support security.

Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G Deployment

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, see the "System Configuration Overview" chapter in the *Cisco Unified Communications Manager System Guide*.

After you have set up the IP telephony system and configured system-wide features in Cisco Unified Communications Manager Administration, you can add IP phones to the system. To add Cisco 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, see the *Cisco Unified Wireless IP phone 7925 and 7926 Series Deployment Guide* at

this URL: http://www.cisco.com/en/US/products/hw/phones/ps379/products_implementation_design_guides_list.html.

Note   The Cisco Unified Wireless IP Phone 7926G must be running Firmware Version 1.4(1) or later.

Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G Setup in Cisco Unified Communications Manager

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

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

For general information about configuring phones in Cisco Unified Communications Manager, see the "Cisco Unified IP Phone" chapter in the *Cisco Unified Communications Manager System Guide*.

Related Topics

Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G Installation

After you have added the phones to the Cisco Unified Communications Manager Administration, you can complete the phone installation. You can install the phone or the user can install the phone. The *Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G Installation Guide* provides directions for assembling the phone and accessories and charging the battery.

Before 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 autoregistration 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 changing the 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, see the readme file for your phone which is located at: http://www.cisco.com/cgi-bin/tablebuild.pl/ip-7900ser-crypto.

Related Topics

VoIP Wireless Network

This chapter provides an overview of the interaction between the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G and other key components of a VoIP network in a wireless local area network (WLAN) environment.

For detailed information, see the *Cisco Unified Wireless IP Phone 7925 and 7926 Series Deployment Guide* : http://www.cisco.com/en/US/products/hw/phones/ps379/products_implementation_design_guides_list.html

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 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.

The following figure shows a typical WLAN topology that enables the wireless transmission of voice for wireless IP telephony.

Figure 2: WLAN with Cisco Unified Wireless IP Phones
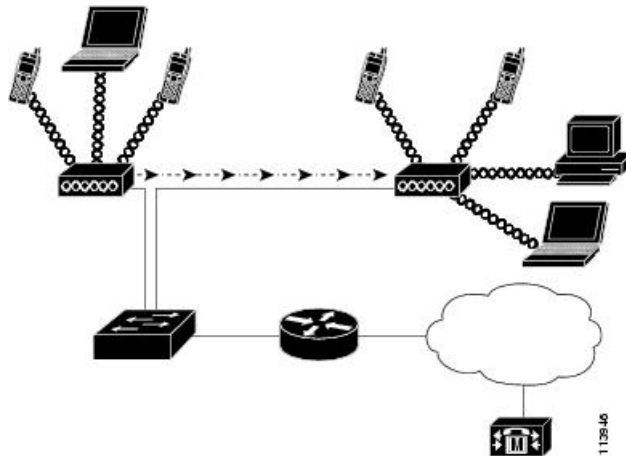
When a wireless IP phone powers up, it searches for and becomes associated with an AP. As users move from one location to another, the wireless IP phone roams out of range of one AP into the range of another AP. The wireless IP phone builds and maintains a list of eligible APs and reconnects to an AP in that list. See AP Association, on page 34 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 transmits 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.

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

For more information on WLANs, APs (including supported models), antennas, and wireless IP telephony, see *Cisco Unified Wireless IP Phone 7925 and 7926 Series Deployment Guide* at http://www.cisco.com/en/US/products/hw/phones/ps379/products_implementation_design_guides_list.html.

WLAN Standards and Technologies

This section describes WLAN standards and technologies.

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 supports the following standards:

802.11a

Uses the 5 GHz band that provides more channels and improved data rates by using Orthogonal Frequency Division Multiplexing (OFDM) technology. Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) supports this standard.

802.11b

Specifies the radio frequency (RF) of 2.4 GHz for both transmitting and receiving data at lower data rates (1, 2, 5.5, 11 Mbps). Commonly called the Wi-Fi standard.

802.11d

Enables APs to communicate available radio channels and acceptable power levels. The Cisco Unified Wireless IP Phone always gives precedence to 802.11d to determine which channels and powers to use. If the information is unavailable, then the phone reverts to the locally configured regulatory domain.

802.11e

Supports Quality of Service (QoS).

802.11g

Uses the same unlicensed 2.4 GHz band as 802.11b, but extends the data rates to provide greater performance by using OFDM technology. OFDM is a physical-layer encoding technology for transmitting signals using RF.

802.11h

Supports the 5 GHz spectrum and transmit power management.

802.11i

Specifies security standards.

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 these devices 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 each section has four channels. The channels are spaced at 20 MHz to provide non-overlapping channels and more channels than 802.11b or 802.11g.

For more information, see the *Cisco Unified Wireless IP Phone 7925 and 7926 Series Deployment Guide*.

The following tables show the frequency band ranges and operating channels by regulatory domain for each of the phones.

Table 4: Cisco Unified Wireless IP Phone 7925G frequency band ranges and operating channels by regulatory domain

Part number	Regulatory domain	Regulatory domain number	Band range	Available channels	Channel set
CP-7925G-A-K9	FCC (Americas)	1050	2.412–2.462 GHz	11	1–11
			5.180–5.240 GHz	4	36, 40, 44, 48
			5.260–5.320 GHz	4	52, 56, 60, 64
			5.500–5.700 GHz	8	100–140
			5.745–5.805 GHz	4	149, 153, 157, 161
CP-7925G-E-K9	ETSI (Europe)	3051	2.412–2.472 GHz	13	1–13
			5.180–5.700 GHz	19	36–48, 52–64, 100–140
CP-7925G-P-K9	Japan	4157	2.412–2.472 GHz	13 (OFDM)	1-13
			2.412–2.484 GHz	14 (CCK)	1-14
			5.180–5.700 GHz	19	36–48, 52–64, 100–140
CP-7925G-W-K9	Rest of World	5252	Uses 802.11d to identify available channels and transmit powers		

Table 5: Cisco Unified Wireless IP Phone 7925G-EX frequency band ranges and operating channels by regulatory domain

Part number	Regulatory domain	Band range	Available channels	Channel set
CP-7925G-EX-K9	5252	2.412–2.484 GHz	14	1–14
		5.180–5.240 GHz	4	36, 40, 44, 48
		5.260–5.320 GHz	4	52, 56, 60, 64
		5.500–5.700 GHz	11	100–140
		5.745–5.805 GHz	4	149, 153, 157, 161

Table 6: Cisco Unified Wireless IP Phone 7926G frequency band ranges and operating channels by regulatory domain

Part number	Regulatory domain	Band range	Available channels	Channel set
CP-7926G-K9	5252	2.412–2.484 GHz	14	1–14
		5.180–5.240 GHz	4	36, 40, 44, 48
		5.260–5.320 GHz	4	52, 56, 60, 64
		5.500–5.700 GHz	11	100–140
		5.745–5.805 GHz	4	149, 153, 157, 161

Note   802.11j (channels 34, 38, 42, 46) and channel 165 are not supported

802.11 data rates, transmit power, ranges, and decibel tolerances

The following table lists the transmit (Tx) power capacities, data rates, ranges in feet and meters, and decibels tolerated by the receiver for the 801.11 standard.

Table 7: Tx power, data rates, ranges, and decibels by standard

Standard	Maximum Tx power (see note 1)	Data rate (see note 2)	Range	Receiver sensitivity
802.11a				

Standard	Maximum Tx power (see note 1)	Data rate (see note 2)	Range	Receiver sensitivity
	16 dBm	6 Mbps	604 ft (184 m)	-91 dBm
		9 Mbps	604 ft (184 m)	-90 dBm
		12 Mbps	551 ft (168 m)	-88 dBm
		18 Mbps	545 ft (166 m)	-86 dBm
		24 Mbps	512 ft (156 m)	-82 dBm
		36 Mbps	420 ft (128 m)	-80 dBm
		48 Mbps	322 ft (98 m)	-77 dBm
		54 Mbps	289 ft (88 m)	-75 dBm
802.11g				
	16 dBm	6 Mbps	709 ft (216 m)	-91 dBm
		9 Mbps	650 ft (198 m)	-90 dBm
		12 Mbps	623 ft (190 m)	-87 dBm
		18 Mbps	623 ft (190 m)	-86 dBm
		24 Mbps	623 ft (190 m)	-82 dBm
		36 Mbps	495 ft (151 m)	-80 dBm
		48 Mbps	413 ft (126 m)	-77 dBm
		54 Mbps	394 ft (120 m)	-76 dBm
802.11b				
	17 dBm	1 Mbps	1,010 ft (308 m)	-96 dBm
		2 Mbps	951 ft (290 m)	-85 dBm
		5.5 Mbps	919 ft (280 m)	-90 dBm
		11 Mbps	902 ft (275 m)	-87 dBm

Note	1	Tx power: Adjusts dynamically when associating with an AP if the AP client setting is enabled.
	2	Data rate: 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 (Cisco Compatible Extensions [CCX] V4) is used.

Wireless Modulation Technologies

Wireless communications use 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 the data packets for the device and all other data packets 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. When used with 802.11g and 802.11a, OFDM can support data rates as high as 54 Mbps.

The following table provides a comparison of data rates, number of channels, and modulation technologies by standard.

Table 8: 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
Nonoverlapping channels	3 (Japan uses 4)	3	Up to 23
Wireless modulation	DSSS	OFDM	OFDM

AP, Channel, and Domain Relationships

APs transmit and receive RF signals over channels within the 2.4 GHz or 5 GHz frequency band. To provide a stable wireless environment and reduce channel interference, you must specify nonoverlapping channels for each AP. The recommended 2.4 GHz channels to be used are 1, 6, and 11.

Regulatory domains determine the number of channels that wireless communications can use within the frequency band. Radio frequency ranges, on page 25 list the frequency ranges, operating channels, and

product numbers for the regulatory domains. The Cisco Unified Wireless IP Phone 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, Cisco recommends that you statically configure channels for each AP. If your wireless network uses a controller, use the Auto-RF feature with minimal voice disruption. Some channels may need to be statically configured if there is an intermittent interferer, to avoid disruptions in that area.

The AP coverage area depends on the type of antenna and transmission power. The AP coverage range is from 500 to 1000 feet with effective isotropic radiated power (EIRP) output. 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, see the "Overview: Cisco Unified Wireless Network" at http://www.cisco.com/en/US/solutions/ns175/networking_solutions_products_genericcontent0900aecd80529a5f.html.

WLANs and roaming

Wireless IP phones provide communication mobility to users within the WLAN environment. Unlike cellular phones that have a 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 up 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 and Layer 3 mobility is not enabled, the phone recognizes that it is no longer in the same subnet. The phone must request a new IP address before it can connect to the network and place the call. If Layer 3 mobility is enabled, the phone does not need to reconnect to the network.

> **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. Pressing a key on the phone causes the phone to perform immediate scans to find and connect 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 reauthenticate with each new AP. See Authentication methods, on page 39 for information about authentication.

If the user is roaming across Layer 2 boundaries, then Layer 3 mobility must be enabled to have seamless roaming, and to preserve an existing call.

If the wireless IP phone user moves from an AP that covers IP Subnet A to an AP that covers IP Subnet B without Layer 3 mobility enabled, 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

Layer 3 roaming is available with Cisco autonomous and unified deployments. With unified deployments, Layer 3 roaming can be performed using intercontroller roaming or, if AP groups are used, to enable Layer 3 roaming.

Layer 3 roaming with Cisco Unified Access Points is accomplished by controllers that use dynamic interface tunneling and requires Layer 3 mobility to be enabled. 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 the CCKM protocol, the wireless IP phone negotiates the handoff from one AP to another easily. During the roaming process, the phone scans for the nearby APs, determines which AP can provide the best service, and then reassociates with the new AP. When implementing stronger authentication methods, such as WPA2 and EAP, the number of information exchanges increases and causes more delay during roaming. To avoid delays, use CCKM.

CCKM, a centralized key management protocol, provides a cache of session credentials on the Cisco Unified Wireless LAN Controller or a 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 off-network or audio gap time.

For details about CCKM, see 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.

Related Topics

Bluetooth Wireless Technology

Bluetooth enables low-bandwidth wireless connections within a range of 30 feet (10 meters). The best performance is in the 3- to 6-foot (1- to 2-meter) range. Bluetooth wireless technology operates in the 2.4 GHz band, which is the same as the 802.11b/g band. Because of potential interference issues, we recommend that you:

- Use 802.11a, which operates in the 5 GHz band

- Reduce the proximity to other 802.11b/g devices, Bluetooth devices, microwave ovens, and large metal objects

VoIP Wireless Network Components

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

For more information, see *Cisco Unified Wireless IP Phone 7925 and 7926 Series Deployment Guide* at http://www.cisco.com/en/US/products/hw/phones/ps379/products_implementation_design_guides_list.html.

Network protocols

Cisco Unified Wireless IP Phones support several network protocols for voice communication. The following table describes the network protocols that the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G supports.

Table 9: Supported network protocols

Network protocol	Purpose	Usage notes
Cisco Discovery Protocol (CDP)	Device-discovery protocol that runs on all Cisco-manufactured equipment. Using CDP, a device advertises its existence to other devices and receives information about other devices in the network.	Cisco Unified Wireless 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.

Network protocol	Purpose	Usage notes
Dynamic Host Configuration Protocol (DHCP)	Dynamically allocates and assigns an IP address to network devices. 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.	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. Use DHCP custom option 150. With this method, you configure the TFTP server IP address as the option value. For additional supported DHCP configurations, see *Cisco Unified Communications Manager System Guide*.
Internet Protocol (IP)	Messaging protocol that addresses and sends packets across the network.	To communicate using IP, network devices must have an assigned IP address, subnet, and gateway. IP addresses, subnet, and gateway identification 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.
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 Wireless IP Phones use the RTCP protocol to allow monitoring of the data delivery and minimal control and identification functionality.
Real-time Protocol (RTP)	Standard for transporting real-time data, such as interactive voice and video, over data networks.	Cisco Unified Wireless IP Phones use the RTP protocol to send and receive real-time voice traffic from other phones and gateways.
Skinny Call Control Protocol (SCCP)	Uses Cisco-proprietary messages to communicate between IP devices and Cisco Unified Communications Manager, Release 4.3 or later.	Cisco Unified Wireless IP Phones use SCCP protocol for VoIP call signaling and enhanced features such as Message Waiting Indication (MWI).
Transmission Control Protocol (TCP)	Connection-oriented transport protocol.	Cisco Unified Wireless IP Phones use TCP to connect to Cisco Unified Communications Manager and to access XML services.
Trivial File Transport Protocol (TFTP)	Method for transferring files over the network. On the Cisco Unified Wireless 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.

Network protocol	Purpose	Usage notes
Transport Layer Security (TLS)	TLS is a standard protocol for securing and authenticating communications.	When security is implemented, Cisco Unified Wireless 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 Wireless IP Phones receive and process UDP messages. RTP voice traffic runs over UDP.

Related Topics

Cisco Unified Wireless AP Interactions

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, passageways and so on.

To ensure good voice quality and optimal RF signal coverage, you must perform a site survey. The site survey determines the AP platform and antenna type, AP placement, channel assignments and transmit power levels that are required for the deployment.

After you deploy and use wireless voice, you should continue to perform postinstallation 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 postinstallation survey verifies that the AP coverage remains adequate for optimal voice communications.

Related Topics

AP Association

At startup, the Cisco Unified Wireless IP Phone 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.

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.

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 *Cisco Unified Wireless IP Phone 7925 and 7926 Series Deployment Guide*.

Related Topics

Voice QoS in Wireless Networks

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 that is typically used for all network devices.

You typically need at least three VLANs on the network switches and the APs that support voice connections on the WLAN. These VLANs are:

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 infrastructure devices

Assign an SSID to the voice VLAN and a different SSID to the data VLAN. 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 the following figure.

Figure 3: Voice traffic in a wireless network
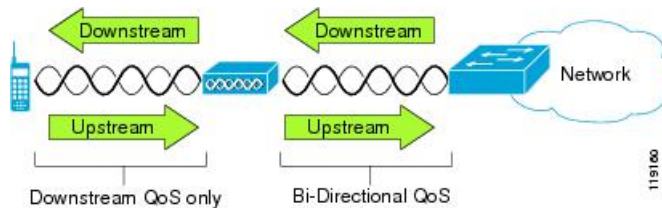
Beginning with Cisco IOS release 12.2(11)JA, Cisco Aironet APs support the contention-based channel access mechanism called Enhanced Distributed Coordination Function (EDCF). The EDCF-type of QoS has up to eight queues for downstream (toward the 802.11b/g clients) QoS. You can allocate the queues based on these options:

- Differentiated Services Code Point (DSCP) settings for the packets

- Layer 2 or Layer 3 access lists

- VLANs for specific traffic

Different traffic types are sent to different priority queues. The following are the queues:

- Best Effort (BE) = 0, 3

- Background (BK) = 1, 2

- Video (VI) = 4, 5

- Video (VO) = 6, 7

Call Control (SCCP) is sent on UP4 (VI) and voice is sent as UP6 (VO).

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 marks the call control packets with a DSCP value of 24 and voice packets with DSCP value of 46.

To improve reliability of voice transmissions in a nondeterministic environment, the Cisco Unified Wireless IP Phone 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 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 Network Busy message. The system maintains a small bandwidth reserve so that wireless phone clients can roam into a neighboring AP, even when the AP is at full capacity. After the AP reaches 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 sets do not need to be modified. To configure QoS correctly on the AP, see *Cisco Unified Wireless IP Phone 7925 and 7926 Series Deployment Guide*.

Related Topics

Cisco Unified Communications Manager Interactions

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 the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G, you must use Cisco Unified Communications Manager Release 4.3 and later, and SCCP.

Before Cisco Unified Communications Manager can recognize a phone, the phone must register with Cisco Unified Communications Manager and be configured in the database.

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

Phone Configuration Files and Profile Files

Phone configuration files 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 the phone to reset, 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 SEP*xxxxxxxxxxxx*.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 Topics

Dynamic Host Configuration Protocol server interactions

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 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, as shown in the following table.

Table 10: DHCP settings priority

Priority	DHCPsettings
1	DHCP option 150
2	DHCP option 66
3	SIADDR
4	ciscoCM1

If DHCP is disabled, the Cisco Unified Wireless IP Phone uses the network settings in the following table to perform the phone provisioning bootup process. You must configure these static parameters for each Cisco Unified Wireless IP Phone.

Table 11: 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 that TCP/IP can distinguish between them.

Static Setting	Description
Default Router 1	Identifies the gateway that provides connectivity to the IP network beyond the subnet to which the phone belongs.
DNS Server 1 DNS Server 2	If the system is configured to use hostnames for servers instead of IP addresses, identifies the primary and secondary DNS server to resolve hostnames.
TFTP Server 1 TFTP Server 2	Identifies the TFTP servers that the phone uses to obtain configuration files.

Voice Communication Security 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 and Cisco Aironet APs are supported in the Cisco SAFE Security architecture. For more information about security in networks, see http://www.cisco.com/en/US/netsol/ns744/networking_solutions_program_home.html.

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 nonencrypted.

Open Authentication with WEP

This is similar to Open Authentication in the preceding bullet, except with improved security. Communication between the wireless device and AP use Wired Equivalent Privacy (WEP) keys to provide security.

Shared Key Authentication

The AP sends an unencrypted challenge text string to any device attempting to communicate with the AP. The device that requests authentication uses a preconfigured WEP key to encrypt the challenge text and sends the encrypted challenge text 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.

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 (PAC) 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. The server and client 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:

- A Wireless LAN client (user machine) requires a valid certificate to authenticate to the WLAN network.

- An authentication server (typically a RADIUS server) requires a server certificate to validate its identity to the clients.

- A Certificate Authority (CA) server infrastructure issues certificates to the authentication 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. This functionality is disabled by default and you enable it using Cisco Unified Communications Manager Administration.

PEAP with Server Certificate Authentication

The Cisco Unified Wireless IP Phone can validate the server certificate during the authentication handshakes over an 802.11 wireless link.

Lightweight Extensible Authentication Protocol (LEAP)

Cisco proprietary password-based mutual authentication scheme between the client (phone) and a RADIUS server. Cisco Unified Wireless IP Phones can use LEAP for authentication with the wireless network.

Auto (AKM)

Selects the 802.11 Authentication mechanism automatically from the configuration information exhibited by the AP. Supports WPA/WPA2-PSK or LEAP with 802.1x+WEP or WPA/WPA2.

This section describes the following concepts:

-
-

Authenticated key management

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

Wi-Fi Protected Access (WPA)

Uses information on a RADIUS server to generate unique keys for authentication. Because these keys are generated at the centralized RADIUS server and are not saved on the phone or AP, WPA provides more security than WPA Pre-Shared Key (WPA PSK). WPA2 provides more security than WPA.

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. The EAP username and password that are used for authentication must be entered on each phone.

Authenticated key management supports WPA/WPA2-PSK and WPA/WPA2/802.1x+WEP utilizing LEAP for the EAP type. CCKM can optionally be used with WPA/WPA2/802.1x+WEP mode.

Encryption methods

To ensure that voice traffic is secure, the Cisco Unified Wireless IP Phone 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 set up on the phone must match the WEP key that is configured at the AP for successful connections. The Cisco Unified Wireless IP Phone 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.

Temporal Key Integrity Protocol (TKIP)

WPA uses 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.

AP authentication and encryption options

Authentication and encryption schemes are set up 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 Cisco Unified Wireless IP Phone.

Some authentication schemes require specific types of encryption. With Open authentication, you can 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, you have several choices for both authentication and encryption setup 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 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 uses network EAP for 802.1x but you can enable open EAP.

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

Table 12: Authentication and encryption schemes

Cisco AP configuration			Cisco Unified Wireless IP Phone 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 WPA	WPA with optional CCKM	TKIP	EAP-FAST

Cisco AP configuration			Cisco Unified Wireless IP Phone configuration
EAP-FAST 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-PSK	WPA-PSK	TKIP	Auto (AKM)
WPA2-PSK	WAP2-PSK	AES	Auto (AKM)

For more information about Cisco WLAN Security, see http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_brochure09186a00801f7d0b.html.

For more information about configuring authentication and encryption schemes on APs, see 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

Site Survey Verification

Before the initial deployment of wireless phones in the WLAN, perform a site survey 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, 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.

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 to view or send to Cisco TAC for troubleshooting purposes.

The following topics provide information about performing the site survey.

Verify wireless voice network

When you perform a site survey verification and encounter problems, see for assistance with finding the cause of the problem.

Perform these tasks to verify wireless voice network operation.

Procedure

Step 1 Check that the wireless IP phone associates with all APs in the WLAN.

Step 2 Check that the wireless IP phone authenticates with all APs in the WLAN.

Step 3 Check that the wireless IP phone registers with Cisco Unified Communications Manager.

Step 4 Check that the wireless IP phone can make stationary phone calls with good quality audio.

Step 5 Check that the wireless IP phone can make roaming phone calls with good quality audio and no disconnections.

Step 6 Check that the wireless IP phone can place multiple calls, especially in areas designated for high density use.

Step 7 After phones are installed, request that users report any problems when using their wireless IP phones.

Related Topics

Display Neighbor List

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 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	AP Name	RSSI	Channel Utilization (CU)
36	ap1	-59	10
149	ap2	-65	2
52	ap3	-70	15

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

```
AP Name: ap1
SSID: voice
Channel: 36
BSSID: 00:13:1a:16:cf:d0
RSSI: -59
CU: 10
```

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 adequate coverage overlap.

Perform Site Survey

Use the Site Survey utility to actively and passively scan the wireless medium across all channels and to locate APs that belong to the Basic Service Set (BSS). The results of the scans can 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.

⚠

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 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 you to view from the phone web page.

Related Topics

Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G Setup

This chapter contains the following topics, which help you install and configure the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G on an IP telephony network:

Before You Begin

Before installing a Cisco Unified Wireless IP Phone, review the requirements in the following sections.

Network Requirements

For the Cisco Unified Wireless IP Phone 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.

- VoIP Network
    - Cisco routers and gateways configured for VoIP

- Either Cisco Unified Communications Manager Release 4.3 or later, or Cisco Unified Communications Manager Express Release 4.3 or later

- IP network configured to support DHCP or manual assignment of IP address, gateway, and subnet mask

Related Topics

Cisco Unified Communications Manager phone addition methods

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. The following table provides an overview of these methods.

Table 13: Phone addition methods for the Cisco Unified Communications Manager Database

Method	Requires MAC address?	Notes
Autoregistration	No	Results in automatic assignment of directory numbers
Autoregistration with the Tool for Auto-Registered Phones Support (TAPS)	No	Requires autoregistration 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.

Autoregistration Phone Addition

Use autoregistration to enter phones into the Cisco Unified Communications Manager database without first gathering MAC addresses from the phones. When autoregistration 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   Autoregistration is disabled by default in Cisco Unified Communications Manager Administration. You must enable and properly configure autoregistration before connecting any Cisco Unified IP Phone to the network. For information about enabling and configuring autoregistration, see *Cisco Unified Communications Manager Administration Guide*.

Autoregistration and TAPS Phone Addition

Use autoregistration 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 predefined 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 autoregistration in Cisco Unified Communications Manager Administration for TAPS to function.

For Cisco Unified Communications Manager Release 5.0 or earlier, see *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 or later, see *Cisco Unified Communications Manager Bulk Administration Guide*.

BAT phone addition

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.

The following table describes how to determine the MAC address of the wireless IP phone.

Table 14: Determine the MAC address of the phone

Method	For more information
Choose **SETTINGS** > **Model Information** > **MAC Address** and look at the MAC Address field.	See View Model Information screen, on page 183
Remove the battery and look on the back of the phone.	See Install or remove phone battery, on page 57

✎

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

For detailed instructions about using BAT, see the following documents:

- For Cisco Unified Communications Manager Release 5.0 and earlier, see *Bulk Administration Tool User Guide for Cisco Unified Communications Manager*.

- For Cisco Unified Communications Manager Release 6.0 and later, see *Cisco Unified Communications Manager Bulk Administration Guide*.

✎

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

Cisco Unified Communications Manager Administration Phone Addition

Add phones individually by using Cisco Unified Communications Manager Administration. To do so, obtain the MAC address for each phone before you begin. See Cisco Unified Communications Manager phone addition methods, on page 50 for instructions.

Perform one of the following after collecting the MAC addresses:

- Cisco Unified Communications Manager Release 5.0 or later: Choose **Device** > **Phone** and click **Add New**.

- Cisco Unified Communications Manager Release 4.x: Choose **Device** > **Add a New Device**.

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

Device Support

Cisco Unified Communications Manager Release 4.3 and later require a device package or service release update installed to enable device support for the Cisco Unified Wireless IP Phone. Device packages including support for the Cisco Unified Wireless IP Phone are available at http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Safety Information

Review the following warnings before installing the Cisco Unified Wireless IP Phone. To see translations of these warnings, see the Regulatory Compliance and Safety Information for the Cisco Unified Wireless IP Phone 7920 Series and Peripherals document that accompanied the device.

Warning   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

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

Warning   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.

Warning   Do not use the Cisco Unified Wireless IP Phone 7925G and 7926G 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.

Warning   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.

Warning   The battery charger used with Cisco Unified IP Wireless Phone 7925G-EX is not ATEX or CSA certified and as such it should not be charged in hazardous environment.

Warning   Use CSA or ATEX qualified Bluetooth accessories with the Cisco Unified IP Wireless Phone 7925G-EX in hazardous environments.

Battery Safety Notices

These battery safety notices apply to the batteries that are approved by the Cisco Unified Wireless IP Phone 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   Ultimate disposal of this product should be handled according to all national laws and regulations. Statement 1040

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 with 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.

⚠️

Caution   To obtain a battery, contact your local dealer. Use only the batteries that have a Cisco part number.

Standard battery

CP-BATT-7925G-STD

Extended use battery

CP-BATT-7925G-EXT

Use only the Cisco power supply that is compatible with your phone. To order your power supply, contact your local dealer and 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=

✎

Note   The battery and power supply are not provided with your phone. To order the battery and power supply, contact your local dealer.

Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G Installation

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. The following sections contain installation information.

Phone power

The Cisco Unified Wireless IP Phone uses a battery for power. The following table lists the types of batteries available for the wireless IP phone and the maximum talk and standby times.

Table 15: Batteries available for the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G

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

When an AP supports the Cisco Compatible 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 50 percent less.

The following table 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 16: Battery charging time

Battery type	Power supply connected to phone	Phone connected to PC and USB cable
Standard	2 hours	5 hours
Extended	3 hours	7 hours

Install or remove phone battery

To install the battery in the wireless IP phone, follow these steps.

Procedure

Step 1 Remove the cover on the back of the phone as shown in the following figure.

Figure 4: Remove cover to install the battery

1	Locking catch
2	Battery cover

Step 2   To install the battery, insert the battery catches in the corresponding slots at the bottom of the Cisco Unified Wireless IP Phone. 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 the following figure.

Figure 5: Install the battery

1	Battery insertion slots
2	Battery

Step 4 To remove the battery, press up on the locking catch, then lift and remove the battery.

Figure 6: Replace the back cover
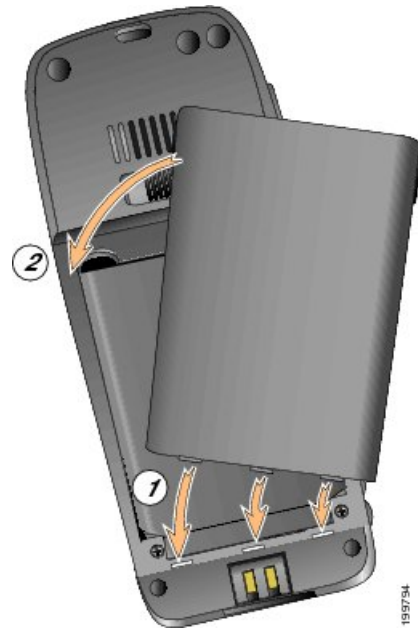
1	Cover insertion slots
2	Cover

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

Charge phone battery using power supply

Use the following figure and steps to charge the phone battery quickly.

Figure 7: Charge the phone battery

Procedure

Step 1 Lift the mini-USB port cover on the bottom of phone.

Step 2 Swing the port cover to one side.

Step 3 Insert the AC power supply mini-USB connector in the port.

Step 4 Insert the AC plug adapter in the slot on the power supply.

Step 5 Insert the AC power supply in a wall outlet.
The indicator light indicates the charging status:

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 Phone power, on page 56.

Charge phone battery using USB cable and PC

The following figure shows how to connect your phone to a PC to charge the phone battery.

Figure 8: Charge the phone battery using the USB cable and PC

Procedure

Step 1 Insert the phone connector on the USB cable into the phone.

Step 2 Insert the USB A-type connector into the USB port on your PC.

Step 3 Monitor the indicator light after the phone briefly displays `USB Connected` on the status line.

Step 4 If you see the `Found New Hardware Wizard` popup message, stop the wizard from opening when connecting to USB port, using the following steps:

a) Click **Next** to use the wizard dialog box.

b) In the Update New Software dialog, click **No, not this time**, and click **Next**.

c) Click **Install the Software automatically (Recommended)** and click **Next**.

d) After a few moments, the Cannot Install This Hardware dialog displays. Click **Don't prompt me again to install this software**.

e) 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 Phone power, on page 56.

Related Topics

Wireless LAN Settings for Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G

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

WLAN Settings from Cisco Unified Wireless IP Phone Web Pages

You can access the Cisco Unified Wireless IP Phone 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.

Related Topics

WLAN Settings from Network Profile Menu on Phone

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.

Related Topics

Headset usage

Although Cisco performs some internal testing of third-party wired and Bluetooth wireless headsets for use with the Cisco Unified Wireless IP Phone, 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.

Warning   Use CSA or ATEX qualified accessories with the Cisco Unified IP Phone 7925G-EX in hazardous environments.

Cisco 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 External device use, on page 64 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 the Cisco Unified IP Phone user. Some humming or buzzing sounds can be caused by a range of outside sources; for example, electric lights, being near electric motors or 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.

Connect headsets

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

Procedure

Step 1 To connect a headset to the Cisco Unified Wireless IP Phone , lift the headset port cover on the right side of the phone.

Step 2 Plug the headset into the headset port.

Bluetooth Wireless Headsets

The Cisco Unified Wireless IP Phone supports Bluetooth Class 2 technology with Hands-Free Profile Version 1.5 when the headsets support Bluetooth. Bluetooth enables low bandwidth wireless connections within a range of 33 feet (10 meters). The best performance is in the 3 to 6 foot (1 to 2 meter) range.

Because of potential interference issues, Cisco recommends 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 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, can affect the connection.

Headset Pairing

The Cisco Unified Wireless IP Phone 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 can be paired with more than one headset at a time. Pairing is typically performed once for each headset.

After a device has been paired, its Bluetooth connection remains as long as both devices (phone and headset) are enabled and within range of each other. The connection reestablishes itself automatically if either of the devices powers down then powers up. The green-dotted Bluetooth icon indicates whether a device is connected.

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

When headsets are more than 10 meters away from Cisco Unified Wireless IP Phone, 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 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 Users should read the headset user guide for more information about pairing and connecting the headsets.

Audio Quality

Beyond the physical, mechanical, and technical performance, the audio portion of a headset must sound good to you (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, 7925G-EX, and 7926G Accessory Guide* and these web sites:

- http://www.plantronics.com

- http://www.jabra.com

- http://www.jawbone.com

External device use

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

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

- Move the external device away from the source of the RF or AF signals.

- Route the external device cables away from the source of the RF or AF signals.

- Use shielded cables for the external device, or use cables with a better shield and connector.

- Shorten the length of the external device cable.

- Apply ferrites or other such devices on the cables for the external device.

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

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

Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G Startup

After charging the battery and configuring the wireless IP phone, you are ready to power on the phone and connect to the WLAN.

To power on the Cisco Unified Wireless IP Phone, 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 has 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.

Related Topics

Active and Standby Phone Modes

The following sections describe the available modes when the Cisco Unified Wireless IP Phone is powered on.

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 keepalive 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 can enter standby mode if none of the events from the Active Mode list are currently active. 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 keepalive packets

Related Topics

Phone startup process

When connecting to the wireless VoIP network, the Cisco Unified Wireless IP Phone goes through a standard startup process, as described in the following list. Depending on your specific network configuration, not all of these steps may occur on your wireless IP phone.

1 Powering on the phone. The Cisco Unified Wireless IP Phone has nonvolatile flash memory in which it stores firmware images and user-defined preferences. At startup, the phone runs a bootstrap loader that loads a phone image stored in Flash memory. Using this image, the phone initializes its software and hardware.

For more information, see and .

2 Scanning for an access point. The Cisco Unified Wireless IP Phone 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.

For more information, see Cisco Unified Wireless AP Interactions, on page 34 and Startup and Connectivity Problems, on page 209.

3 Authenticating with access point. The Cisco Unified Wireless IP Phone begins the authenticating process.

- 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**, **EAP-FAST**, or **PEAP**, the username and password are authenticated by the RADIUS server before network access is available.

- If set for **EAP-TLS**, the phone requires one or more of the following certificates:

  ◦ a client certificate and the RADIUS root certificate

  ◦ the CA certificate

- If set for **Auto (AKM)**, the phone looks for an access point with one of the following key management options enabled:

  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.

  For more information, see Authentication methods, on page 39.

4 Configuring IP network. 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.

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.

For more information, see:

- DHCP Settings, on page 123

- Disable DHCP, on page 123

- Startup and Connectivity Problems, on page 209

5 Downloading Load ID. The wireless IP phone checks to verify that the proper firmware is installed or if new firmware is available to download.

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.

For more information, see Phone Configuration Files and Profile Files, on page 37.

6 Downloading configuration file. 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.

For more information, see:

- Set alternate TFTP server, on page 124
- Phone Configuration Files and Profile Files, on page 37
- Startup and Connectivity Problems, on page 209

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.

For more information, see:

- Cisco Unified Communications Manager Interactions, on page 37
- Startup and Connectivity Problems, on page 209

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 autoregistration is enabled in Cisco Unified Communications Manager, the phone attempts to autoregister itself in the Cisco Unified Communications Manager database.

For more information, see:

- Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G Deployment, on page 19
- Add Users to Cisco Unified Communications Manager, on page 172

Related Topics

Cisco Unified Wireless IP Phones Setup in Cisco Unified Communications Manager, on page 149
Phone Configuration Files and Profile Files, on page 37

Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G Web Pages

This chapter describes how to set up your PC to configure a Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G by using a USB connector and how to remotely access a configured phone over the WLAN. It contains the following sections:

PC setup for phone setup

To set up 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.

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 32 bit
- Windows XP 32 bit
- Windows 7 32 bit
- Windows 7 64 bit

Related Topics

Backup Settings area, on page 107

Install USB drivers

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

Procedure

Step 1 Log in to 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 installation file (listed in the read me 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 When you see the Finished screen, the installation is complete. 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 box 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 to 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 completes.
The phone briefly displays `USB Connected` on the status line.

Set up USB LAN on PC

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

Procedure

Step 1 To set up the USB LAN connection, access the Network Connections window on your PC.

Step 2 Locate and double-click the new LAN connection to open the Local Area Connection Status window, and 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.xxx, where xxx is 1-99 or 101-254.

Example:

192.168.1.11

| **Note** | • By default, the Cisco Unified Wireless IP Phone 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

Access 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 Home web page summary information, on page 75 for details about this web page.

Step 3 When prompted, enter your username and password.

Default username: *admin*

Default password: *Cisco*

Step 4 Use the hyperlinks in the left column of the web page to configure settings for the phones.

Step 5 After entering the new settings, disconnect the USB cable from the phone. The settings are active immediately.

Step 6 Check that the phone can access the network successfully.

Related Topics

Set up phone using USB cable

You are ready to use the USB cable to set up other phones. Before plugging the USB cable into another phone, wait approximately 12 to 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.
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 Access phone web page, on page 71.

Related Topics

Remote Phone Updates

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

Use the following sections for information about remotely updating phones.

Set privileges for 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 in to Cisco Unified Communications Manager Administration.

Step 2 Search for the phone by choosing **Device** > **Phone** and enter search information such as the DN.
Note   The administrator password for web access can also be changed using the Product Specific Configuration page of the Cisco Unified Communications Manager Administration.

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:

a) In the Web Access field, select **Full** from the drop-down menu.

b) 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.

Access phone configuration web page

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

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 Release 5.0 or later, the Phone Configuration web page password might be set to *Cisco*.

To access the web page for the Cisco Unified Wireless IP Phone follow these steps.

Procedure

Step 1 Log in to 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 parameter gives you full access to all of the web pages.

Step 6 Choose one of the following methods:

a) 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). Home web page menu, on page 74 describes the available Home web page menus, from which you can configure network profiles, USB settings, trace settings, Wavelink settings, and certificates. Home web page summary information, on page 75 describes the phone summary information.

b) 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

Step 7 If the Security Alert dialog box displays a notice to accept the Trust Certificate, click **Yes** or **Always** to accept the application.

Step 8 Log in to 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 9 Make changes to configurable pages as needed.

Step 10 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 11 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.

Home web page menu

The following table describes the menu entries in the home web page.

Table 17: Home web page menus

Menu	Related information
Setup	
Network Profiles	Network Profiles, on page 76
USB Settings	Set up USB settings on PC, on page 97
Trace Settings	Set up Trace Settings, on page 98
Wavelink Settings	Set up Wavelink Settings, on page 101
Certificates	Wireless LAN security, on page 82
Configurations	
Phone Book	Phone Book Setup, on page 102
Information	
Network	Home web page summary information, on page 75
Wireless LAN	
Device	
Statistics	
Wireless LAN	Displays Rx and Tx statistics.
Network	Displays IP, TCP, and UDP statistics.

Menu	Related information
Stream Statistics	
Stream 1	Displays RTP statistics and voice quality metrics.
Stream 2	
System	
Trace Logs	System Settings, on page 106
Backup Settings	
Phone Upgrade	
Change Password	
Site Survey	
Date and Time	
Phone Restart	

Home web page summary information

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. The following table describes these items.

Table 18: 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	

Item	Description
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 Unified CM	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

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 Access phone web page, on page 71, and then click the **Network Profiles** hyperlink.

For more information about configuring network profiles, see the following sections.

Network profile settings

You can configure the profile settings using this web page area. You can also modify or view configured profiles from this web page area. The following table describes 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 Access phone web page, on page 71, and then click the **Profile (1-4)** hyperlink.

Table 19: 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.	AP Association, on page 34
Edit Profile	Enables editing of the profile.	
Call Power Save Mode	Set for the type of power saving mode used in the WLAN. Options are: • U-APSD/PS-Poll • None	802.11 Standards for WLAN Communications, on page 24

Item	Description	For more information, see …
802.11 Mode	Determines the signal mode or priority for selecting signal modes available in the WLAN. Options are: • 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) **Note** The preferred band, if available, is 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. After the phone has connected to the less-preferred band, it does not scan for the preferred band if the current band is acceptable, and may remain connected to the less-preferred band. • Auto, signal strength (RSSI): Use strongest signal in dual-band environment	802.11 Standards for WLAN Communications, on page 24
Scan Mode	**Note** Scan Mode is set in the Cisco Unified Communications Manager Administration, and cannot be set from the phone. The phone displays the current setting. Auto: Always scans when on a call. If idle and signal strength is sufficient, the phone does not scan. Continuous: Always scans. Single AP: Only scans at power-on or if the AP connection to the network is lost.	AP Association, on page 34

Item	Description	For more information, see …
Restricted Data Rate	**Note** Restricted Data Rate is set in the Cisco Unified Communications Manager Administration, and cannot be set from the phone. The phone displays the current setting. Enables or disables the restriction of the upstream and downstream PHY rates according to Cisco Compatible Extension (CCX) V4 Traffic Stream Rate Set IE (S54.2.6). The default is disabled.	
WLAN Security		
Security Mode	Assigns the security mode	Set up Advanced Profile settings, on page 96
Export Security Credentials	Controls whether the wireless security credential data can be exported in the configuration file. • True: Allows exporting the data • False: Blocks exporting the data	
Wireless Security Credentials		
Username	Assigns the network authentication username for this profile	Set up username and password, on page 85
Password	Assigns the network authentication password for this profile	
Prompt Mode	**Note** Available only for Network Profile 1. If enabled, then the user must enter the password when powering on the phone. If disabled, the password is saved to the phone memory, and the user does not need to enter the password when powering on the phone.	
WPA Pre-shared Key Credentials		
Pre-shared Key Type	Determines the key type: Hex or ASCII	Pre-shared key setup, on page 85

Item	Description	For more information, see …
Pre-shared Key	Identifies the key	
Wireless Encryption		
Key Type	Determines the encryption key type: Hex or ASCII	Wireless Encryption, on page 86
Encryption Key 1-4	Identifies the Transmit Key: • Encryption Key character string • Key Size of 40 or 128 characters	
Certificate Options		
Client EAP-TLS Certificate	Determines the certificate used for authentication: • Manufacturing issued • User installed	EAP-TLS Authentication Certificates, on page 88
Validate Server Certificate	Enables the phone to use the server certificate. Two options: true or false. **Note** Applies to PEAP only.	
IP Network Configuration		
Obtain IP address and DNS servers automatically	Gets the IP address and DNS servers automatically.	IP Network Settings, on page 94
Use the following IP address and DNS servers	Disables DHCP and uses these static settings: • IP Address • Subnet Mask • Default Router • Primary DNS • Secondary DNS • Domain Name	
TFTP		

Item	Description	For more information, see …
Obtain TFTP Servers Automatically	Enables automatic assignment of TFTP servers	Set up alternate TFTP server, on page 95
Use the following TFTP servers	Assigns static TFTP server IP addresses to: • TFTP Server 1 • TFTP Server 2	
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 uses 802.11b, the PHY rate must be configured to the supported rate.	Set up Advanced Profile settings, on page 96
Surplus Bandwidth	Excess bandwidth beyond application requirements	
802.11G Power Settings		
Channel	Assigns the channels	Set up Advanced Profile settings, on page 96
Status	Enabled: Identifies enabled channels in WLAN to improve scanning for the phone.	
MaxTxPower	Sets the maximum transmit power for the phone	
802.11A Power Settings		
Channel	Assigns the channels	Set up Advanced Profile settings, on page 96
Status	Enabled: Identifies enabled channels in WLAN to improve scanning for the phone	

Item	Description	For more information, see …
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 cannot access the WLAN.

Related Topics

Access phone web page, on page 71

Wireless LAN security, on page 82

Wireless Security Credentials, on page 85

Wireless Encryption, on page 86

Set up wireless settings in network profile

You must configure wireless settings in a profile to enable the phone to access the wireless network. To configure the wireless settings, see Network profile settings, on page 77 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.

Wireless LAN security

The Cisco Unified Wireless IP Phone 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 or 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 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.

Server validation can optionally be enabled from the phone web page in the Network Profile configuration.

The server validation feature requires that the server certificate be imported to the phone from the phone web page.

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 (PSK), WPA2-PSK, 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-PSK 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 use 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. The following table provides a list of supported authentication and encryption schemes that you can configure on the Cisco Unified Wireless IP Phone.

Table 20: 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	Requires a WEP key
Shared Key plus WEP	Static WEP Requires WEP Key	Requires a WEP key
LEAP (with optional CCKM)	Uses WEP, TKIP or AES	Requires Username and Password
EAP-FAST (with optional CCKM)	Uses WEP, TKIP or AES	Requires Username and Password
EAP-TLS (with optional CCKM)	Uses WEP, TKIP, or AES	Requires Username and Password Requires server and client certificates
PEAP (with optional CCKM)	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

Set up 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 Wireless LAN security, on page 82 for more information. |

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

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 the format: *domain\username*. |

The following sections provide information about setting security credentials.

Set up 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 are 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.

Pre-shared key setup

When using Auto (AKM) for WPA Pre-shared key or WPA2 Pre-shared key 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 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 enter 64 hex digits (0-9 and A-F); for example, AB123456789CD01234567890EFAB123456789CD01234567890EF3456789C

ASCII

For ASCII keys, you 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, GREG12356789ZXYW

Set up PSK

To set up a PSK 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 hexadecimal digits in the Passphrase/Pre-shared key field. See Pre-Shared Key Formats, on page 85.

Step 4 Click **Save** to make the change.

Wireless Encryption

If your wireless network uses WEP encryption, and you 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 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 use one of the following key sizes:

40-bit

You enter a 10-digit encryption key string that uses the hex digits (0-9 and A-F); for example, ABCD123456.

128-bit

You enter a 26-digit encryption key string that uses the hex digits (0-9 and A-F); for example, AB123456789CD01234567890EF.

ASCII

For ASCII keys, you enter a character string that uses 0-9, A-Z (upper and lower case), and all symbols, with one of the following key sizes:

40-bit

You enter a 5-character string; for example, GREG5.

128-bit

You enter a 13-character string; for example, GREGSSECRET13.

Set up WEP 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 WEP Key Formats, on page 86.

Step 6   Click **Save** to make the change.

Related Topics

EAP-TLS Authentication Certificates

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 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 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 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 certificates 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) is generated on the phone, sent to the CA for approval, and the approved certificate installed on the Cisco Unified Wireless IP Phone.

During EAP-TLS authentication, the ACS server verifies the trust of the phone and the phone verifies the trust of the ACS server.

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

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

Install EAP-TLS authentication certificates

To install authentication certificates for EAP-TLS, perform the following steps.

Procedure

Step 1 From the phone web page, set the Cisco Unified Communications Manager date and time on the phone. For more information, see Set date and time, on page 89.

Step 2 If using the Manufacturing Installed Certificate (MIC):

a) From the phone web page, export the CA root certificate and manufacturing CA certificate.

b) From Internet Explorer, install certificates on the Cisco ACS server and edit the trust list.

c) From Microsoft Certificate Services, export the CA certificate from the ACS server and import it to the phone.
For more information, see:

- Export and install certificates on ACS, on page 90

- Export CA certificate from ACS using Microsoft Certificate Services, on page 90

Step 3 If using a user installed certificate, from phone web page:

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 phone.
For more information, see Request and import user-installed certificate, on page 91.

Step 4 Using the ACS configuration tool, set up the user account.
For more information, see:

- Set up ACS user account and install certificate, on page 92

- *User Guide for Cisco Secure ACS for Windows*

Set date and time

EAP-TLS uses certificate-based authentication that requires the internal clock on the Cisco Unified Wireless IP Phone 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. Cisco recommends 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**, and then click **OK**.

Export and install certificates on ACS

To use the MIC, export the Manufacturing Root Certificate and Manufacturing CA Certificate and install it on 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**.

Step 2 Click **Export** next to the Manufacturing Root Certificate.

Step 3 Save the certificate and copy it to the ACS server.

Step 4 Repeat Steps 1 and 2 for the Manufacturing CA certificate.

Step 5 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 6 Use the Edit the Certificate Trust List (CTL) page to add the certificates to be trusted by ACS.

ACS Certificate Export Methods

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 .

- To export the CA certificate from the ACS server that uses a self-signed certificate, see .

Export CA certificate from ACS using Microsoft Certificate Services

Use this method to export 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.

Export CA certificate from ACS using Internet Explorer

Use this method to export 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.

Step 4 Click **Next**.

Step 5 At the next window, select **DER encoded binary X.509 (.CER)**, and click **Next**.

Step 6 Specify a name for the certificate and click **Next**.

Step 7 Save the CA certificate to be installed on the phone.

Request and import 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 username in the ACS server. See Set up ACS user account and install certificate, on page 92.

Step 3 Enter the information to be displayed on the certificate, and click **Submit** to generate the Certificate Signing Request (CSR).

Step 4 In the next screen, select and copy the entire contents of the text box (the encoded CSR text). Send this data to the CA administrator for signing.

Send the CSR text 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 5 From the Microsoft Certificate Services Request a Certificate page, select **Advanced certificate request** to initiate the signing request.

Step 6 At the Advanced Certificate Request page, select **Submit a certificate request by using a base-64-encoded PKCS CMC**.

Step 7 Copy the certificate data from the Cisco Unified Wireless IP Phone and paste it in the Saved Request text box, then click **Submit**.

Step 8 After the CSR is approved, the certificate must be exported in a DER encoded format and sent to the original requestor.

Step 9 Return to the phone web page and choose **Certificates** to import the signed certificate.

Step 10 On the Certificates page, locate the User Installed certificate line, and click **Import**.

Step 11 Browse to the certificate on your PC to import to the phone.

Install Authentication Server Root Certificate

To install the Authentication Server Root Certificate on the phone, follow these steps.

Procedure

Step 1 Export the Authentication Server Root Certificate from the ACS. See .

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.

Set up ACS user account and install certificate

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 Request and import user-installed certificate, on page 91.

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.

PEAP Setup

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.

- The Allow EAP-MSCHAPv2 setting must be enabled.

- 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).

Enable 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 Set up Authentication Mode, on page 84.

Step 2   Enter a user name and password.

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.

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.

Related Topics

Enable 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 the option **Obtain IP address and DNS servers automatically**.

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

Disable 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 **Use the following IP addresses and DNS servers**.

Step 3 Enter the required IP addresses. See Network Configuration fields when DHCP not in use, on page 95 for descriptions of these fields.

Step 4 Click **Save** to make the change.

Network Configuration fields when DHCP not in use

When DHCP is not in use, the fields listed in the following table need to be statically configured.

Table 21: Network Configuration fields

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

Set up alternate TFTP server

If you use DHCP to direct the phones 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 the option **Use the following TFTP servers**.
Step 3	You must enter the required IP addresses. See for descriptions of these fields.
Step 4	Click **Save** to make the change.

Set up Advanced 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, Cisco recommends 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, so that 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, so that 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

Set up USB settings on PC

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 Access phone web page, on page 71, 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:

- **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 mask.

Step 5   Click **Save** to make the change.

Related Topics

Set up Trace Settings

You can use the Trace Settings area on the web page to configure how the phone creates and saves trace files (often used in troubleshooting). 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. Trace Settings fields, on page 100 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 Access phone web page, on page 71, and then click the **Trace Settings** hyperlink under Setup. For information about the fields, see Trace Settings fields, on page 100.

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.

There are various levels of tracing available that provide different levels of messaging:

- Emergency

- Alert

- Critical

- Error

- Warning

- Notice

- Info

- Debug

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, 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

- Java

- Bluetooth

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.

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

Trace Settings fields

Table 22: Trace Settings fields

Item	Description
General	
Number of Files	Choose the number of trace files that the phone saves, from 2 to 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 to 65535)
Module Trace Level	
Kernel	Operating System data
Wireless LAN Driver	Channel scanning, roaming, and authentication
Wireless LAN Manager	WLAN Management, QoS
Configuration	Phone configuration, firmware upgrade
Call Control	Cisco Unified Communications Manager messaging (SCCP)
Network Services	DHCP, TFTP, CDP, WWW, Syslog
Security Subsystem	Application level security data
User Interface	Key strokes, softkeys, MMI data
Audio System	RTP, SRTP, RTCP, DSP data
System	Event Manager
Java	Java MIDP
Bluetooth	Bluetooth
Advanced Trace Settings	

Item	Description
Preserve Logs	True: Save trace logs after powering off the phone False: Delete trace logs
Reset Trace Settings upon Reboot	You can enable debugging by configuring various settings on the Trace Configuration. These options determine how trace settings are handled when you reboot: • Yes: Default value. Settings will be reset to the default values upon reboot. • No: Trace settings will not reset upon reboot.

Related Topics

Set up Wavelink Settings

The Cisco Unified Wireless IP Phone supports the use of the Wavelink Avalanche server to configure the phone, which can be set up as a Wavelink Avalanche client device. Configuration Utility for Wavelink Avalanche can be installed on the Wavelink Avalanche server to configure a single phone or multiple phones with common settings. For more information, see Wavelink Avalanche Server, on page 135.

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 identifies a device as a Cisco Unified Wireless IP Phone 7925G or Cisco Unified Wireless IP Phone 7925G-EX, while CP7926 identifies a device as a Cisco Unified Wireless IP Phone 7926G.

By default, the parameters are configured as follows:

• ModelName = CP7925 or CP7926

• EnablerVer = 3.11-01

Note For more information about using the Wavelink Avalanche server, see Wavelink Server IP Address Setup, on page 136.

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.

Phone Book Setup

Cisco Unified Wireless IP Phone 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.

Related Topics

Import and export 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, and 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 displays. Save this file to your PC or another storage device.

Import and export CSV phone contacts

When you export or import phone contact records using the Comma Separated Values (CSV) format, you can view, edit, or create records with third-party software such as Microsoft Excel and Microsoft Outlook. After editing or creating records, you can transfer them to the Cisco Unified Wireless IP Phone.

Note The Cisco Unified Wireless IP Phone 7920G CSV files can be imported into the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G.

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 do not map to Microsoft Outlook by default:

- Nickname
- IM Address
- Unique Identifier (UUID)

Because the importing file may not have the UUID field generated by the Cisco Unified Wireless IP Phone, 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 and 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. Because 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 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 page of the Cisco Unified Wireless IP Phone.

Step 2 Select the **PHONE BOOK** menu.

Step 3 To import, click the **Import** option.

Step 4 Specify how old and duplicated contact records are processed.

Step 5 Click **Create File of Type**.

Step 6 Click **Comma Separated Values (CSV) format**.

Step 7 To export, click the **Export** option.
 Note If a Security Alert window displays, click **Yes**.

Step 8 Click **Open**, **Save**, or **Cancel**.

Step 9 Click **Save** and specify the filename and location.

Step 10 Click **Save** again.

Step 11 Click **Import** after all options are specified.

Step 12 Check the Status web page because it displays the number of valid records that were processed. Because the import function duplicates UUIDs and names, the total number of created contacts on the phone may be less than the total number of records processed.

Search Phone Book

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.

Phone Book Actions

You can update the information for Phone Book from the phone web page.

✎

Note When you enter phone numbers, the web page stores and displays only numeric characters and the symbols **#** and *****.

Add 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 .

Step 4 When finished, click **Save**.

Delete 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**.

Step 3 To delete all contacts, click **DeleteAll**.

Edit 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 Assign speed-dial hot key to contact number, on page 106.

Step 4 When finished, click **Save**.

Assign speed-dial hot key to 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 Add contact, on page 105 or Edit contact information, on page 106.

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**.

Step 5 To change a speed dial assignment, click the speed dial icon again and repeat Step 3.

System Settings

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

Related Topics

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 Cisco 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 display the Trace Logs area, access the web page for the phone as described in the PC setup for phone setup, on page 69, and click the **Trace Logs** hyperlink.

Related Topics

Backup Settings area

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 Access phone configuration web page, on page 73, and click the **Backup Settings** hyperlink. The following table describes the items in this area.

Table 23: Backup Settings area items

Item	Description
Import Configuration	
Encryption Key	Enter the alphanumeric string from 8 to 20 characters long for encrypting the phone settings.
Import File	Enter the path and filename or use the Browse button to locate the file.

Item	Description
Import button	Click the button to import the phone settings file into the phone.
Export Configuration	
Encryption Key	Enter the alphanumeric string from 8 to 20 characters long for encrypting the phone settings.
Export button	Click the button to export the phone settings file to a location on your PC or other location.

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.

Create phone 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 Access phone web page, on page 71.

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 from 8 to 20 characters long.
Record this key because you must enter this key to import the configuration template on other phones.

Step 6 Click **Export**. The File Download dialog box appears.

Step 7 Click **Save**.

Step 8 Give your configuration a new file name, such as *7925template.cfg*.

Step 9 Choose a location on your PC or on the network for the file and click **Save**.

Encrypted Configuration File Contents

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

- 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)

Import 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 Access phone web page, on page 71.

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

Upgrade 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.

Procedure

Step 1 To display the Phone Upgrade area, access the web page for the phone as described in the Access phone configuration web page, on page 73, and click the **Phone Upgrade** hyperlink.

Step 2 To upgrade the phone software, enter the phone software TAR (firmware filename) or use the **Browse** button to locate the firmware file on the network.

Related Topics

Administration Password Changes

The method you use to change an administration password depends on the communications server being used in your system.

Administration Passwords and Cisco Unified CallManager Release 4.x

If you are running Cisco Unified CallManager Release 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 Access phone configuration web page, on page 73, and click the **Change Password** hyperlink in the System submenu.

Administration Passwords and Cisco Unified Communications Manager Release 5.0 or Later

If you are running Cisco Unified Communications Manager Release 5.0 or later, you must set the password in Cisco Unified Communications Manager Administration on the Phone Configuration page. The password that you set in Cisco Unified Communications Manager takes precedence over the password that you set on the web pages.

⚠

Caution When setting the Administration Password in the Product Specific Configuration section in Cisco Unified Communications Manager Release 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

Site Survey Report

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 Perform Site Survey, on page 46.

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 Access Points (AP) displays.

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 Display Neighbor List, on page 45.

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.

The following table shows the information shown in the site survey report.

Table 24: Site Survey Report neighbor table

Information	Description or indicator
Report title	The Service Set Identifier (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): • Percentage of time it is the best AP. • Received Signal Strength Indicator (RSSI) range during the time it is the best AP. **Note** A low number (below -65) may indicate insufficient overlap between the best AP and its neighbors.

Information	Description or indicator
Immediate Neighbor	Information may be displayed in the following way: • Pink background: If AP is on the same channel as the best AP. **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 with other immediate neighbors. • Asterisk (*): Not an immediate neighbor. Information displayed in cell (for example, 27%-61/-39): • Percentage of time the AP is the immediate neighbor of the best AP. • RSSI range during the time the AP is the immediate neighbor.

The following table lists the information that is provided in the AP details report.

Table 25: 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 nth beacon is a delivery traffic indication message (DTIM) period. After each DTIM beacon, the AP sends 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.
BSS Lost Count	The Basic Service Set (BSS) Lost Count increments when the phone passes a threshold number of missed beacons. Missed beacons identify synchronization problems.

Field	Description
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 microseconds per second.
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: • None • WEP40 • WEP104 • TKIP • CCMP • CKIP CMIC • CKIP • CMIC
AKM	One or more of the following: • 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.

Field	Description
WMM Supported	Support for Wi-Fi Multimedia Extensions.
CCX Version Number	Version of CCX if the AP is CCX compliant.
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 Best Effort AC Video AC Voice AC	Access Category information for each AC: • 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.
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 with 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 with the reference AP for consistency.

CHAPTER **5**

Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G Settings

This chapter describes the available configuration settings on the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G. It contains the following sections:

Access Settings menu

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

✎

Note   You can control whether a Cisco Unified Wireless IP Phone 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 Product-specific fields for Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G, on page 163.

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, perform 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 ⬛, press **** #** on the keypad to unlock the option.

When the menu is unlocked, ⬛ displays.

Related Topics

Network Profile Settings

On the Cisco Unified Wireless IP Phone, 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 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.

The following sections provide information about configuring network profiles.

Related Topics

Access Network Profile menu

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

Procedure

Step 1   Choose **SETTINGS** > **Network Profiles**.

Step 2   To select the profile name that you want to configure, perform 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 .

Step 3   To unlock the network settings in the profile, press * * #.

The option unlocks, and displays.

Step 4   To display the profile settings, press **View**.

Step 5   Scroll to and select one of these menu options:

• **Profile Name**

• **Network Configuration**

• **WLAN Configuration**

Step 6   Make changes to the settings. For more information, see

Step 7   To save changes to settings in the Profile menu, press **Save**.

Step 8   To use the modified profile, scroll to the profile name and press **Select**. The appears beside the enabled profiles. You can enable up to four profiles.

Change 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 make 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 **View** 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. For information on input restrictions, see Network Profile data input guidelines, on page 120.
Step 6	Press **Options** > **Save** to complete the name change.

Network Profile data input guidelines

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 uppercase).

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 0 to enter a space between characters.

Enter a dot

Press 0 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 0 to enter a space **+ , . ' " | _ ~ '**
- Press # to enter **# ? ( ) [ ] { }**
- Press 1 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

Network settings

After accessing a network profile, you can use the following table for descriptions and reference information for network profile settings.

Table 26: 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.	DHCP Settings, on page 123
MAC Address	Unique MAC address of the phone.	Display only, cannot configure
Host Name	Unique hostname 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.	DHCP Settings, on page 123

Network setting	Description	For more information, see..
IP Address	Internet Protocol (IP) address of the phone.	DHCP Settings, on page 123
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.	
Alternate TFTP	Yes: This option assigns an alternative Trivial File Transfer Protocol (TFTP) server. No: This option uses the TFTP server assigned by DHCP.	Set alternate TFTP server, on page 124
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 nonzero value for this option.	
TFTP Server 2	Optional backup TFTP server that the phone uses if the primary TFTP server is not available.	
Load Server	IP address for the server where the phone receives firmware updates.	*Cisco Unified Communications Manager Administration Guide*
CDP Enabled	Enables or disables Cisco Discovery Protocol (CDP) for the phone in Cisco Unified Communications Manager Administration.	Change Cisco Discovery Protocol settings, on page 125 *Cisco Unified Communications Manager Administration Guide*
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.	Product-specific fields for Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G, on page 163

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.

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 an alternate TFTP server.

Related Topics

Dynamic Host Configuration Protocol server interactions, on page 38

Disable 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 **Edit**.
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 **Options** > **Cancel**.
Step 9	After you disable DHCP, you must enter the other required static fields. See Static settings with disabled DHCP, on page 124 for descriptions of these fields. For information about entering values, see Network Profile data input guidelines, on page 120.

Static settings with disabled DHCP

Table 27: 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.
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 hostnames for servers instead of IP addresses, identify the primary and secondary DNS server to resolve hostnames.
Alternate TFTP server	Identifies whether you are using an alternate TFTP server. See Set alternate TFTP server, on page 124.
TFTP Server 1	Identifies the TFTP server that the phone uses to obtain configuration files.
TFTP Server 2	Identifies the second TFTP server that the phone can use to obtain configuration files.

Set alternate TFTP server

If you use DHCP to direct the phones 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 press the **View** 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 Static settings with disabled DHCP, on page 124 for descriptions of these fields.

For information about entering values, see Network Profile data input guidelines, on page 120.

Step 8 Press **Options** > **Validate** to save the entry or press **Options** > **Cancel**.

Change 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 Scroll to **Device Information**.

Step 4 Scroll to **Cisco Discovery Protocol (CDP)**.

Step 5 Click **Enabled** from the drop-down menu.

Step 6 Click **Save** and **Reset**, if prompted.

Erase network profile 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 press the **View** 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

WLAN Configuration Settings

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.

The following sections contain information about configuring wireless settings.

Access WLAN Configuration menu

To access the WLAN Configuration menu options on a Cisco Unified Wireless IP 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 press the **View** 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 WLAN Configuration fields, on page 126.

Step 6 Press **Options** > **Save** to save the entry or press **Options** > **Cancel**.

WLAN Configuration fields

After accessing the WLAN settings, use the following table for descriptions and reference information for these settings.

Table 28: WLAN Configuration settings

Network setting	Description	For more information, see...
SSID	Unique identifier for accessing wireless access points.	Network Profiles, on page 76

Network setting	Description	For more information, see...
Security Mode	The type of authentication that the phone uses to access the WLAN. Options are: **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).	Wireless LAN security, on page 82

Network setting	Description	For more information, see...
UserName	Username for the wireless network (up to 32 characters).	Set up username and password, on page 85
Password	Password for the wireless network (up to 32 characters).	Set up username and password, on page 85
Key Style (Available when Security Mode is AKM, Open+WEP, or Shared+WEP)	Specifies the format for the key. • HEX • ASCII	
Pre-shared Key (Available when Security Mode is AKM)	Enter the Pre-shared key in the field provided.	
Static WEP Key 1 Static WEP Key 2 Static WEP Key 3 Static WEP Key 4 (Available when Security Mode is Open+WEP or Shared+WEP)	Specifies the length of the static WEP key. • 40 Bits • 128 Bits	
802.11 Mode	The wireless signal standard used in the WLAN. Options are: • 802.11b/g • 802.11a • Auto-b/g • Auto-a • Auto-RSSI	802.11 Standards for WLAN Communications, on page 24
Call Power Save Mode	The type of power saving mode used in the WLAN. Options are: • U-APSD/PS-Poll • None	Network protocols, on page 32

Network setting	Description	For more information, see...
Prompt Mode (Available for Network Profile 1, when Security Mode is LEAP, EAP-FAST, PEAP, or Auto AKM)	Sets the prompt mode to one of the following options: • Enable • Disable	

Related Topics

Phone Settings Menu

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

Note You can control whether a Cisco Unified Wireless IP Phone 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.

Related Topics

Set up Phone Settings

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

Procedure

Step 1 Choose **SETTINGS** > **Phone Settings**.

Step 2 Press the number for the setting that you want to configure or scroll to the setting and press the **Select** button.

Step 3 Press the number for the setting category or scroll to the setting and press the **Select** button.

Step 4 Press the number for the setting that you want to change or scroll to the setting and press the **Select** button. For descriptions of the settings, see Phone Settings fields, on page 130. For specific instructions to change these settings, see "Configure Phone Settings" in the *Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G User Guide*.

Phone Settings fields

The following table describes the fields in the Phone Settings page.

Table 29: Configurable settings for the phone sounds, display, and keypad

Phone setting	Description
Sound Settings	
Ring Tone	Assigns the ringtone for each line on the phone. **Current Settings** Provides a list of ring tones that you can listen to. **Available Ring Tones** Provides a list of ring tones.
Volumes	Contains the following submenu entries: **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.

Phone setting	Description
Display Timeout	Sets the length of time for the phone screen to display before turning off or disables the timer so screen always displays. • 10 Seconds • 30 Seconds • 1 Minute • 2 Minutes
LED Coverage Indicator	Enables or disables the LED blink to indicate that the phone is in service and within the coverage area.
Font Size	Sets the size of font used on the display. • Default • Increased
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. • Disable • 15 Seconds • 30 Seconds • 60 Seconds
Keypad Tone	Enables or disables tones for keypad presses. • Disable • Normal • Loud
Customize Home Page	
Left Softkey	Sets the phone to display Message or Phone Book as the left softkey on the home page.
Background Image	Sets the background image that the phone displays.
Bluetooth	
Bluetooth	Enables or disables Bluetooth functions.

Phone setting	Description
Device List	Displays the list of Bluetooth devices available to the phone.
Diagnostics	
Keypad	Performs a diagnostic routine to check a button on the keypad.
Audio	Causes the phone to ring to check the speaker.
WLAN	Checks the WLAN.
Scanner (Cisco Unified Wireless IP Phone 7926G only)	Checks the bar code scanner.

Related Topics

Set up phone security certificate

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 associated with the Certificate Authority Proxy Function (CAPF). You can use Cisco Unified Communications Manager Administration to configure an LSC, as described in the *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 must 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.

For more information on certificates, see *Cisco Unified Communications Manager Security Guide*. For more information about the security features, see Security features, on page 14.

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 **Update**.
The phone prompts for an authentication string.

Step 5 Enter the authentication string and press **Submit**.
The phone begins to install, update, or remove the LSC, depending on how the CAPF was configured. During the procedure, a series of messages 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 **Stop** from the Security Configuration menu. Settings must be unlocked before you can press this softkey.

When the phone successfully completes the installation procedure, it displays `Success`. If the phone displays `Failed`, the authorization string may be incorrect or the phone may not be enabled for upgrading. See the error messages generated by the CAPF and take appropriate actions.

Step 6 To verify that an LSC is installed on the phone, choose **SETTINGS** > **System Configuration** > **Security**.
The LSC displays `Installed`.

Related Topics

Change USB port setup

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 your area.

To view or configure the USB port configuration on a Cisco Unified Wireless IP Phone, 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** 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 Steps 5 through 12.

Note   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**.

Step 6   Enter a new IP address that is not assigned on the subnet.

Step 7   To save the changes, press **Options** > **Save**.

Step 8   To change the subnet for the new IP address, scroll to **Subnet Mask** and press **Select**.

Step 9   Enter the appropriate subnet address.

Step 10   To save the changes, press **Save**.

Related Topics

CHAPTER **6**

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, 7925G-EX, and 7926G. The Configuration Utility (CU) for Wavelink Avalanche can be installed on the Wavelink Avalanche Management Console and used to configure a single phone or multiple phones with common settings.

Note   The phones do not support Traffic Stream Rate Set (TSRS) or Cisco Compatible Extensions (CCX) V4.

Note   Not all features can be configured using Wavelink. Some features can only be configured from Cisco Unified Communications Manager Administration.

This chapter contains the following sections:

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, 7925G-EX, and 7926G Firmware Release 1.3(1) or later

• Configuration Utility (CU) for Wavelink Avalanche

• DHCP server

• Cisco Unified Communications Manager

Best Practices

This section describes the best practices recommended for setting up and using the 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 has access only to the Wavelink server.

• Configure DHCP Option 149 with the Wavelink server IP address. If you do not configure this option, see .

• Configure a Cisco Access Point to use a default SSID of "cisco" with open authentication and no encryption.

Wavelink Server IP Address Setup

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.

The following sections describe the methods to assign the Wavelink server on the phone.

Set up Wavelink server address from phone

To assign the Wavelink server from the phone, follow these steps.

Procedure

Step 1	Turn on the phone.
Step 2	Verify that the phone is installed with the required firmware version and is registered to Cisco Unified Communications Manager.
Step 3	Choose **SETTINGS** > **System Configuration** > **Wavelink**.
Step 4	To unlock the phone, press ****#**.
Step 5	In the Alternate Wavelink Server option, choose **Yes**.
Step 6	Enter the IP address of the Wavelink server, and press **Save**.

Set up Wavelink server address from 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.
Step 3	Click **Save**.

Set up and use CU

This section describes the tasks for configuring and using the CU from the Wavelink Management Console.

Note The CU is labeled as 7921G but the CU works for all 792X phones.

To set up and use the CU from the Wavelink Management Console, perform the following tasks.

Procedure

Step 1	Assign attributes for the phone. For more information, see Phone Attributes Setup, on page 138.
Step 2	Install the CU on Wavelink. For more information, see Install CU file, on page 139.
Step 3	Update the configuration files. For more information, see Update configuration files, on page 139.
Step 4	Update the phones. For more information, see Phone Attributes Setup, on page 138.

Phone Attributes Setup

You can assign attributes on the Cisco Unified Wireless IP 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 field of CP7925G is used to identify a device as the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G.

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, use the following sections to define values for the CustomName and CustomValue fields.

Define CustomName and CustomValue on 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.

Define custom parameters from 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.

Install CU file

The CU file is provided by Cisco in the .ava file format.

Note Install the CU on the Wavelink Avalanche Management Console.

For more information, see the Wavelink Avalanche Management Console documentation.

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 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 completes, 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. The following additional steps are optional. They 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**, and then click **Test Expression**.

Step 12 Review the list displayed under Matching Clients to ensure the selection criteria have been met.

Step 13 Click **Apply**, then click **OK**.

Update configuration files

You can update a phone configuration file using the CU installed on a Wavelink Avalanche Management Console.

The following table lists the configuration file settings.

Table 30: Configuration file settings

Setting	For more information, see...
Profile Settings	Profile Settings fields, on page 140
WLAN Settings	
Network Settings	
USB Settings	USB Settings Field, on page 145
Trace Settings	Trace Settings fields, on page 145
Wavelink Settings	Wavelink settings fields, on page 146

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**
- **Wavelink Settings**

Step 3 From the settings page, select or enter information for those settings.

Step 4 Click **Apply**.

Profile Settings fields

The following table lists the fields in the Profile Settings screen.

Table 31: 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**.	

Item	Description	For more information, see …
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.	
WLAN Mode	Determines the signal mode or priority for selecting signal modes available in the WLAN. Options are: • 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) **Note** The preferred band, if available, is 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. After the phone has connected to the less-preferred band, it does not scan for the preferred band if the current band is acceptable, and will remain connected to the less-preferred band. • Auto, signal strength (RSSI): Use strongest signal in dual-band environment	802.11 Standards for WLAN Communications, on page 24
Call Power Save Mode	Set for the type of power saving mode used in the WLAN. Options are: • U-APSD/PS-Poll • None	802.11 Standards for WLAN Communications, on page 24
WLAN Security		

Item	Description	For more information, see …
Authentication Mode	Sets the authentication and encryption methods for this profile: **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: • 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	
Password	Assigns the network authentication password for this profile	

Item	Description	For more information, see …
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: **40 bits** 5 ASCII or 10 hexadecimal characters **128 bits** 13 ASCII or 26 hexadecimal characters	
Network Settings		
DHCP Enabled	**Yes** Enables DHCP to obtain IP address and DNS servers automatically. **No** DHCP is disabled and you will need to enter the following fields: • IP Address • Subnet Mask • Default Router • Primary DNS • Secondary DNS • Domain Name	

Item	Description	For more information, see …
TFTP		
Alternate TFTP	Determines whether DHCP assigns the TFTP server. If yes, enter static IP addresses for: • 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	• Vertical • Horizontal • Diversity	
Antenna Selection for 802.11B	• 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.

Related Topics

USB Settings Field

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.

Related Topics

Trace Settings fields

You can configure trace settings to determine how the phone creates and saves trace files. The following table describes the trace settings.

Table 32: Trace Settings

Item	Description
Number of Files	Choose the number of trace files that the phone saves, from 2 to 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.
Kernel Level	Operating System data.
Configuration Level	Phone configuration data.
Call Control Level	Cisco Unified Communications Manager data.

Item	Description
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.

Wavelink settings fields

You can configure Wavelink settings from the phone CU. The following table describes the Wavelink settings.

Table 33: 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.

Update 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 CU does not perform a complete validation of the phone configuration. If the configuration file contains an invalid setting, the phone may 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 CU, select the configuration file, and 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)**.

Step 4   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 actions:

- Choose **Update Now**.

- Choose **Client Settings**. In the Avalanche Client Controls window, check the **Force package sync during Update Now** check box, and click **Update Now**.

Features, Templates, Services, and Users

This chapter provides an overview of the feature configuration and setup, softkey template modification, services setup, and user assignment in Cisco Unified Communications Manager Administration. Cisco Unified Communications Manager documentation provides detailed instructions for these procedures.

For suggestions about providing users with information for using the phone and features, see Internal Support Website, on page 231. For information about setting up phones in non-English environments, see International User Support, on page 235.

This chapter contains the following sections:

Cisco Unified Wireless IP Phones Setup in Cisco Unified Communications Manager

To provide telephony call routing and call-control features for the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G, you must use Cisco Unified Communications Manager Administration. For instructions about adding these devices, see the "Cisco Unified IP Phone Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*.

Telephony features available

The following table describes supported telephony features that you can configure using Cisco Unified Communications Manager Administration for the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G. The table provides references to documentation that contains configuration procedures and feature information.

For information about using the features on the phone, see *Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G User Guide for Cisco Unified Communications Manager*.

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 34: Telephony features for the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G

Feature	Description	Configuration Reference
7926G J2ME Memory Increase	Increases the amount of Java MIDP memory available for the Cisco Unified Wireless IP Phone 7926G.	No configuration required.
792x USB Driver Support for Microsoft Windows 7	Enables USB driver support for Microsoft Windows 7.	No configuration required.
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.	For more information, see: *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Configuration" chapter *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phone" chapter
Auto Answer	Connects incoming calls automatically after a ring or two to the speakerphone or headset if attached.	For more information, see the *Cisco Unified Communications Manager Administration Guide*: - For Cisco Unified Communications Manager Release 5.0 or later, see the "Configuring Directory Numbers" chapter - For Cisco Unified Communications Manager Release 4.x, see the "Phone Configuration" chapter

Feature	Description	Configuration Reference
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, see *Cisco Unified Communications Manager Features and Services Guide*, "Call Pickup Group Configuration" chapter.
Barge	Allows a user to join a nonprivate call on a shared phone line. Barge features include cBarge, Barge, and Single Button Barge. • cBarge adds a user to a call and converts it into a conference, allowing the user and other parties to access conference features. • Barge adds a user to a call but does not convert the call into a conference. • Single Button Barge enables users to Barge or cBarge into a remote-in-use call on a shared line. The phones support Barge in two conference modes: • Built-in conference bridge at the target device (the phone that is being barged). This mode uses the **Barge** softkey. • Shared conference bridge. This mode uses the **cBarge** softkey. **Note** The Barge and Privacy features work together.	For more information, see: • *Cisco Unified Communications Manager Administration Guide*, "Device Pool Configuration" chapter • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones" chapter • *Cisco Unified Communications Manager Features and Services Guide*, "Barge and Privacy" chapter
Block external to external transfer	Prevents users from transferring an external call to another external number.	For more information, see *Cisco Unified Communications Manager Features and Services Guide*, "External Call Transfer Restrictions" chapter.
Busy Lamp Field (BLF) speed dial	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 do not disturb (DND). During the alerting state, call pickup capability is enabled. **Note** This feature is not supported in Cisco Unified Communications Manager Release 4.x.	For more information, see *Cisco Unified Communications Manager Features and Services Guide*, "Presence" chapter.
Call Back	Provides users with an audio and visual alert on the phone when a busy or unavailable party becomes available.	For more information, see: • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones" chapter • *Cisco Unified Communications Manager Features and Services Guide*, "Call Back" chapter

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, see: • *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Configuration" chapter • *Cisco Unified Communications Manager System Guide*, "Understanding Route Plans" chapter • *Cisco Unified Communications Manager Features and Services Guide*, "Call Display Restrictions" chapter
Call forward	Allows users to redirect incoming calls to another number. Call forward options include Call Forward All, Call Forward Busy, Call Forward No Answer, and Call Forward No Coverage.	For more information, see: • *Cisco Unified Communications Manager Administration Guide*, "Directory Number Configuration" chapter • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones" chapter • Customize User Options web page display, on page 173
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, see the *Cisco Unified Communications Manager System Guide*, "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 Forward Maximum Hop Count service parameter allows.	For more information, see the *Cisco Unified Communications Manager System Guide*, "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, see: • *Cisco Unified Communications Manager Administration Guide* • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones" chapter

Feature	Description	Configuration Reference
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, see *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones" chapter.
Call park	Allows users to park (temporarily store) a call and then retrieve the call by using another phone in the Cisco Unified Communications Manager.	For more information, see: • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones" chapter • *Cisco Unified Communications Manager Features and Services Guide*, "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 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 and visual alert is only available for phones on Cisco Unified Communications Manager Release 4.2 and later.	For more information, see: • *Cisco Unified Communications Manager Features and Services Guide*, "Call Pickup Group Configuration" chapter • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones" chapter • *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Configuration" chapter
Call waiting	Indicates (and allows a user to answer) an incoming call that rings while the user is on another call. Displays incoming call information on the phone screen.	For more information, see: • *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Configuration" chapter (Release 4.x) • Cisco Unified *Communications Manager Administration Guide*, "Directory Number Configuration" chapter (Release 5.x and later) • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones" chapter

Feature	Description	Configuration Reference
Caller ID	Displays caller identification such as a phone number, name, or other descriptive text on the phone screen.	For more information, see: • *Cisco Unified Communications Manager Administration Guide*, "Configuring Cisco Unified IP Phones" chapter • *Cisco Unified Communications Manager System Guide*, "Understanding Route Plans" chapter • *Cisco Unified Communications Manager Features and Services Guide*, "Call Display Restrictions" chapter
Calling Party Normalization	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. To globalize a DN, use the international escape character, plus (+).	For more information, see: • *Cisco Unified Communications Manager Features and Services Guide*, "Calling Party Normalization" chapter • *Cisco Unified Communications Manager System Guide*, "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, see the *Cisco Unified Communications Manager Features and Services Guide*, "Client Matter Codes and Forced Authorization Codes" chapter.
Conference	Allows a user to talk simultaneously with multiple parties by calling each participant individually. Conference features include Conference, Join, cBarge, and Meet-Me. Allows a noninitiator in a standard (ad hoc) conference to add or remove participants; also allows any conference participant to join together two standard conferences on the same line. The Service parameter, AdvanceAdhocConference, (disabled by default in Cisco Unified Communications Manager Administration) allows you to enable these features. **Note** Be sure to inform your users if these features are activated.	For more information, see: • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones" chapter • *Cisco Unified Communications Manager System Guide* "Conference Bridges" chapter

Feature	Description	Configuration Reference
Configurable call forward display	Allows you to specify information that appears on a phone when a call is forwarded. This information can include the caller name, caller number, redirected number, and original dialed number.	For more information, see: • Cisco Unified Communications Manager 5.0 or later—*Cisco Unified Communications Manager Administration Guide*, "Directory Number Configuration" chapter • Cisco Unified Communications Manager 4.x—*Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Configuration" chapter • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones" chapter
Direct transfer	Allows a user to connect two calls to each other (without remaining on the line).	For more information, see *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones" chapter.
Directed Call Park	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. 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. **Note** If you implement Directed Call Park, avoid configuring the Park softkey. This prevents users from confusing the two Call Park features.	For more information, see *Cisco Unified Communications Manager Features and Services Guide*, "Call Park and Directed Call Park" chapter.
Do Not Disturb (DND)–Reject	Enables a user to temporarily stop incoming calls 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.	For more information, see *Cisco Unified Communications Manager Features and Services Guide*, "Do Not Disturb" chapter.
Dock Icon Support for Cisco Unified Wireless IP Phone 7925G Desktop Charger	An icon displays on the phone screen when the phone is docked in the desktop charger. The phone must be already paired with the desktop charger.	No configuration required.

Feature	Description	Configuration Reference
DND	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. You can configure the phone to have a softkey template with a DND softkey or a phone-button template. **Note** DND is available in Cisco Unified Communications Manager 6.0 or later. The following DND parameters are configurable in Cisco Unified Communications Manager Administration: **DND** This check box 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.	For more information, see: • *Cisco Unified Communications Manager Features and Services Guide*, "Do Not Disturb" chapter • *Cisco Unified Communications Manager Administration Guide*
Extension Mobility	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.	For more information, see: • *Cisco Unified Serviceability Administration Guide* • *Cisco Unified Communications Manager Features and Services Guide*, "Cisco Unified Communications Manager Extension Mobility" chapter • *Cisco Unified Communications Manager Business Edition*, "Cisco Extension Mobility" chapter

Feature	Description	Configuration Reference
Fast Dial Service	Allows a user to enter a Fast Dial code to place a call. Fast Dial codes can be assigned to phone numbers or Personal Address Book entries.	For more information, see *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phone Services" chapter.
Forced authorization codes (FAC)	Controls the types of calls that certain users can place.	For more information, see *Cisco Unified Communications Manager Features and Services Guide*, "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, see *Cisco Unified Communications Manager Features and Services Guide*, "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.
Hold Reversion	Limits the amount of time that a call can be on hold before reverting back to the phone that put the call on hold and alerting the user. Reverting calls are distinguished from incoming calls by a single ring (or beep, depending on the new call indicator setting for the line). This notification repeats at intervals if the call is not resumed. A call that triggers Hold Reversion displays a brief message on the status line. You can configure call focus priority to favor incoming or reverting calls.	For more information about configuring this feature, see *Cisco Unified Communications Manager Features and Services Guide*, "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.	For more information, see: • *Cisco Unified Communications Manager Administration Guide*, "Hunt Group Configuration" chapter • *Cisco Unified Communications Manager System Guide*, "Understanding Route Plans" chapter

Feature	Description	Configuration Reference
Immediate Divert	Allows a user to transfer a ringing, connected, or held call directly to a voice-messaging system.When a call is diverted, the line becomes available to make or receive new calls.	For more information, see: • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones" chapter • *Cisco Unified Communications Manager Features and Services Guide*, "Call Park and Directed Call Park" chapter
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, see: • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones" chapter • *Cisco Unified Communications Manager Features and Services Guide*, "Immediate Divert" chapter
Intercom	Allows users to place and receive intercom calls from the line view. You can configure intercom lines to: • 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, see: • *Cisco Unified Communications Manager Feature and Services Guide*, "Intercom Configuration" chapter • *Cisco Unified Communications Manager Feature and Services Guide*, "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, see *Cisco Unified Communications Manager System Guide*, "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, see *Cisco Unified Communications Manager System Guide*, "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 nonhunt group calls from ringing their phones.	For more information, see *Cisco Unified Communications Manager System Guide*, "Understanding Route Plans" chapter.

Feature	Description	Configuration Reference
Malicious caller identification (MCID)	Allows users to notify the system administrator about suspicious calls that are received.	For more information, see: • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones" chapter. • *Cisco Unified Communications Manager Features and Services Guide*, "Malicious Call Identification" chapter.
Meet Me conference	Allows a user to host a Meet Me conference in which other participants call a predetermined number at a scheduled time.	For more information, see *Cisco Unified Communications Manager Administration Guide*, "Meet-Me Number/Pattern Configuration" chapter.
Message waiting indicator	A light on the handset that indicates that indicates that a user has one or more new voice messages.	For more information, see: • *Cisco Unified Communications Manager Administration Guide*, "Message Waiting Configuration" chapter • *Cisco Unified Communications Manager System Guide*, "Voice Mail Connectivity to Cisco Unified Communications Manager" chapter
MIDlet Minimize to Background When Power On	Enables the phone to automatically start a Java MIDlet in the background when the phone powers on.	Java MIDlet startup, on page 170
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, see *Cisco Unified Communications Manager Features and Services Guide*, "Multilevel Precedence and Preemption" chapter.
Music on hold	Plays music while callers are on hold.	For more information, see *Cisco Unified Communications Manager Features and Services Guide*, "Music On Hold" chapter.
Onhook call transfer	Allows a user to press a single Transfer softkey and then go on-hook to complete a call transfer.	For more information, see *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones" chapter.
Other group pickup	Allows a user to answer a call ringing on a phone in another group that is associated with the user's group.	For more information, see *Cisco Unified Communications Manager Features and Services Guide*, "Call Pickup Group Configuration" chapter.

Feature	Description	Configuration Reference
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, see *Cisco Unified Communications Manager Features and Services Guide*, "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, see: • *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Configuration" chapter • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones" chapter • *Cisco Unified Communications Manager Features and Services Guide* "Barge and Privacy" chapter
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 Services Menu, on page 168. Requires an XML application to provide Push to Talk service.
Quality Reporting Tool (QRT)	Allows users to use the **QRT** softkey on a phone to submit information about problem phone calls. QRT can be configured for either of two user modes, depending upon the amount of user interaction desired with QRT.	For more information, see: • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones" chapter • *Cisco Unified Communications Manager Features and Services Guide*, "Quality Report Tool" chapter
Redial	Allows users to call the most recently dialed phone number by using a softkey option.	Requires no configuration.

Feature	Description	Configuration Reference
Ring setting	Identifies ring type used for a line when a phone has another active call.	For more information, see: • Cisco Unified Communications Manager Release 4.x: *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Configuration" chapter • Cisco Unified Communications Manager Release 5.x or later: *Cisco Unified Communications Manager Administration Guide*, "Configuring Directory Numbers" chapter • *Cisco Unified Communications Manager Features and Services Guide*, "Custom Phone Rings" chapter. • Custom Phone Rings Creation, on page 174
Services	Allows you to use the Cisco Unified IP Phone Services Configuration menu in Cisco Unified Communications Manager Administration to define and maintain the list of phone services to which users can subscribe.	For more information, see: • *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Configuration" chapter • *Cisco Unified Communications Manager System Guide*, "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, see *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones" chapter.
Speed dial	Dials a specified number that has been previously stored. Speed dialing includes these features: • 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.	For more information, see: • *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Configuration" chapter • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones" chapter

Feature	Description	Configuration Reference
Time-of-Day Routing	Restricts access to specified telephony features by time period.	For more information, see: • *Cisco Unified Communications Manager Administration Guide*, "Time Period Configuration" chapter • *Cisco Unified Communications Manager System Guide*, "Time-of-Day Routing" chapter
Timezone Support	Enables Java MIDlets to use the time zone information configured on the phone from the Cisco Unified Communications Manager.	For more information, see *Cisco Unified Communications Manager System Guide*.
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, see: • *Cisco Unified Communications Manager Administration Guide*, "Cisco Voice-Mail Port Configuration" chapter • *Cisco Unified Communications Manager System Guide*, "Voice Mail Connectivity to Cisco Unified Communications Manager" chapter
XSI Audio Path Control	Enables XSI calls to specify if the audio is played on the speakerphone or handset speaker. For more information, see the *Cisco Unified IP Phone Services Application Development Notes*.	No configuration required.

Related Topics

Product-specific fields for Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G

Each Cisco Unified IP Phone has special configuration fields in Cisco Unified Communications Manager Administration that are available by phone model. The following product-specific configuration fields are available for the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G.

Table 35: Product-specific fields

Parameter	Options	Description
Disable Speakerphone	True or False	Turns off the speakerphone capability of the handset.
Gratuitous ARP	Enable or disable	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.
Settings Access	Enabled, Disabled, and Restricted	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, the Settings menu does not display any options.
Web Access	Read Only, Full, Disabled	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.
Profile 1-4	Unlocked or locked	Locks or unlocks the network profiles. If locked, the phone user cannot modify the network profile.
Load Server	IP address or hostname for the server	Identifies the alternate server that the phone uses to obtain firmware loads and upgrades.
Admin Password (Cisco Unified Communications Manager Release 5.0 and later)	8 to 32 characters long Default: "CiscoCisco"	Password to access the configuration web pages for the phone. **Caution** When setting the Administration Password in the Product Specific Configuration section in Cisco Unified Communications Manager Administration Release 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	up to 16 digits in length	Identifies special phone numbers that do not require unlocking the keypad to call, such as 911 or an emergency number
Application URL	maximum length is 256 characters	Specifies the URL that the phone uses to contact application services.
"Send" Key Action	Enable or Disable	When enabled, pressing the green button causes the phone to go off-hook. When disabled, pressing the green button causes the phone to display the list of recently dialed numbers (for last number redial).

Parameter	Options	Description
Phone Book Web Access	Enabled or Disabled	Controls the access of the local phone book so that it can be accessed by using the web page for the phone. This parameter works with the Web Access parameter. When Web Access is disabled, the local phone book is not accessible.
Unlock-Settings Sequence (**#)	Enabled or Disabled	Specifies the unlock settings as **#. If this parameter is enabled, the phone cannot be unlocked using any other key sequence. 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	Time in seconds	Specifies the amount of time to hold down the Application button to activatee the application.
Application Button Priority	Low, Medium, High	Indicates the priority of the Application button relative to the other phone tasks. **Low** Specifies that the Application button works only when the phone is idle and on the main screen. **Medium** Specifies that the button takes precedence over all tasks except when the keypad is locked. **High** 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 one time or regularly at 10, 30, or 60 second intervals. When the phone is within range of an AP, the alert stops.
Scan Mode	Auto, Single AP, Continuous Default: Auto	Controls the scanning by the phone. **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.
Restricted Data Rates	Enable or disable Default: disabled	Enables or disables the restriction of the upstream and downstream PHY rates according to CCX V4 Traffic Stream Rate Set IE (S54.2.6).

Parameter	Options	Description
Power Off When Charging	Enable or disable Default: disabled	Indicates whether the phone powers off when it is connected to a charger or placed in a charging station.
Cisco Discovery Protocol	Enable or disable Default: enabled	Enables or disables the Cisco Discovery Protocol on the phone.
Advertise G.722 Codec	Use System Default, Disabled, Enabled Default: Use System Default	Indicates whether the phone advertises the G.722 codec to the Cisco Unified Communications Manager. Codec negotiation involves two steps: **1** The phone must advertise the supported codec to the Cisco Unified Communications Manager (not all endpoints support the same set of codecs). **2** 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. **Enabled** Advertises G.722 to the Cisco Unified Communications Manager.
Home Screen	Main Phone Screen or Line View Default: Main Phone Screen	Enables one of two views on the phone: Main Phone Screen or Line View.
FIPS Mode	Enable or disable Default: disabled	Enables or disables the Federal Information Processing Standards (FIPS) mode on the phone.
Auto Line Select	Enable or disable Default: disabled	Enables or disables the Auto Line Select feature on the phone. If enabled, the phone shifts the call focus to incoming calls on all lines. If disabled, the phone shifts only the call focus to incoming calls on the currently used line.
Bluetooth	Enable or disable Default: enabled	Enables or disables the Bluetooth option on the phone. If disabled, the user cannot enable Bluetooth on the phone.
File System Verification	Enable or disable Default: disabled	Enables the phone to perform a file system integrity check as part of the firmware upgrade process. This parameter is used to troubleshoot file system issues. Enabling this feature may affect phone performance.

Parameter	Options	Description
Bar Code Symbology Group	Basic or extended Default: basic	Specifies the symbology the scanner uses to scan barcodes. Select either basic or extended depending on the barcode types being used. Available only on the Cisco Unified Wireless IP Phone 7926G.
Scanner Commands		Allows you to specify multiple commands for barcode scanner features. For more information, see the *Java MIDlet Developers Guide for Cisco Unified IP Phones* and the *Cisco IP Phone Services MIDlet Software Development Kit*. Available only on the Cisco Unified Wireless IP Phone 7926G.
Minimum Ring Volume	Default: 0	If a user does not have access to the phone configuration menus, this setting controls the minimum ring volume a user can adjust the volume to.

Set up product-specific options

To configure product-specific options, follow these steps.

Procedure

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

Step 2 Perform one of the following actions:

- For Cisco Unified Communications Manager 4.x or earlier, click **Add a Phone**.

- For Cisco Unified Communications Manager 5.0 and later, click **Add Phone**.

Step 3 Choose **Phone Type** > **Cisco7925**.

Step 4 In the Phone Configuration page, locate the **Product Specific Configuration** area.

Step 5 Make changes to the settings as needed. See Product-specific fields for Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G, on page 163 for a description of the fields.

    Note For detailed information about these settings, click the **I** or **?** button for Product Specific Configuration Help.

Step 6 Check the **Override Common Settings** check box to override higher level configuration settings for that feature.

Step 7 Reset the phone to make the changes take effect.

Softkey Templates

Administrators can change the order of softkeys for the Cisco Unified Wireless IP Phone 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 has two nonconfigurable softkeys that are set for:

- Message

- Options

When you configure a softkey template for the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G, you can configure the Cisco Unified Communications Manager softkeys and their sequence in the Options menu only. 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.

Standard and Nonstandard Softkey Templates

The standard softkey template displays the Hold softkey when a call is connected. Some users want the Transfer softkey to appear for a connected call instead of Hold.

To change the softkey that displays, you set up a nonstandard softkey template that places Transfer in the first position for the Connected state. You assign this nonstandard softkey template to the Cisco Unified Wireless IP Phone 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.

Softkey Template Setup

Use the procedures in the online Help topic, "Adding Non-Standard Softkey Templates" to change the softkeys and their sequence. Softkey templates support up to 16 softkeys for 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. For more information, see the "Softkey Template Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide* and the *Cisco Unified Communications Manager System Guide*.

Related Topics

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, see the "Cisco Unified IP Phones" chapter in the *Cisco Unified Communications Manager System Guide* for your release.

The Cisco Unified Wireless IP Phone can have up to six lines and up to 24 connected calls. The default button template uses position 1 for lines and assigns positions 2 through 6 as speed dial. You can assign the following 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, and conferencing.

Services Menu

The Services menu on the Cisco Unified Wireless IP Phone gives users access to Cisco Unified IP Phone Services. These services are XML applications or Java MIDlets 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 that is located on the side of the phone.

To create customized XML applications for your site, see the Cisco Unified IP Phone Service Application Development Notes.

Before a user can access any service, two important tasks must be completed:

- 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.

Note   For information about extension mobility services for users, see the "Cisco Extension Mobility" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

Related Topics

Product-specific fields for Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G, on page 163

Set up IP Phone services

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 Perform one of the following actions:

- To set up these services in Cisco Unified Communications Manager Administration for Release 4.x, choose **Feature** > **Cisco IP Phone Services**.

- To set up these services in Cisco Unified Communications Manager Administration for Release 5.0 or later, choose **Device** > **Device Settings** > **Phone Services**.

For more information about phone services, see the "Cisco Unified IP Phone Services" chapter in the *Cisco Unified Communications Manager System Guide*.

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 User Phone Features and Services, on page 233 for a summary of the information that you must provide to end users.

Java MIDlet Support

The Cisco Unified Wireless IP Phone supports the use of Java MIDlets offered by Cisco vendors and third-party developers. Running Java MIDlet applications directly on the phone allows more sophisticated application capabilities than with existing XML services, such as animated graphics, custom user interface objects, advanced network connectivity, and persistent local storage. Because Java MIDlets are an industry standard, developers can use standard Java development tools for building applications.

Cisco Unified Communications Manager IP Phone Service provisioning and subscription interfaces allow explicit provisioning of IP Phone Services using the phone configuration file. This explicit provisioning system allows Java MIDlet applications to be installed and managed on the phone. When a new service is added in the configuration, the phone downloads and installs it. When a service is removed, the phone uninstalls it.

For more information on Java MIDlets, see the *Java MIDlet Developers Guide for Cisco Unified IP Phones* and the *Cisco IP Phone Services MIDlet Software Development Kit*.

Java MIDlet startup

You can enable a Java MIDlet to automatically launch when a phone powers on.

For a MIDlet to automatically launch, the phone must subscribe to the MIDlet application. If the phone is not subscribed to the MIDlet, the automatic launch fails.

To configure a MIDlet to automatically launch, you configure the Idle URL field in the Phone Configuration window of the Cisco Unified Communications Manager Administration with URL to the MIDlet in the following format:

```
<MIDlet URL> -minimize
```

Note The `-minimize` must have a space *before* the hyphen, and there must be no space *after* the hyphen.

The Idle URL Timer field is not used by the launched URL.

When the phone powers on and registers with the Cisco Unified Communication Manager, the MIDlet automatically launches and minimizes to the background. The user can close the MIDlet manually while the phone is powered on. After the MIDlet is closed, the user can manually launch the MIDlet at a later time or turn the phone off and on to restart the MIDlet.

For more information, see the *Cisco Unified Communications Manager Administration Guide* and the *Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G User Guide*.

Example

To automatically launch the WifiScanner MIDlet, configure the Idle URL field with the following information:

```
http://<ip address>/MIDlets/WifiScanner.jad -minimize
```

where `<ip address>` is the IP address of the server that stores the MIDlet.

Corporate and Personal Directories

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

Corporate Directory

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

Personal Directory

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

Corporate Directory

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 interact 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, see 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 you configure the LDAP directory, users can use the Corporate Directory service on the Cisco Unified Wireless IP Phone to look up users in the corporate directory.

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. For details, see .

Cisco Unified IP Phone Address Book Synchronizer

Make sure to provide users with the installer for this application.

Obtain Cisco Unified IP Phone Address Book Synchronizer application

To obtain the installer, follow these steps.

Procedure

Step 1 Choose **Application** > **Plugins** > **Installation** from Cisco Unified Communications Manager Administration.

Step 2 Click **Download**, which is located next to the **Cisco Unified IP Phone Address Book Synchronizer** plugin name.

Step 3 When the file download dialog box displays, click **Save**.

Step 4 Send the TabSyncInstall.exe file to all users who require this application.

Add 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 one of these methods:

- To add users individually from Cisco Unified Communications Manager Administration for Release 5.0 or later, choose **User Management** > **End User** > **Add New**.

  See "Adding a New User" chapter in *Cisco Unified Communications Manager Administration Guide* for more information about adding users. See *Cisco Unified Communications Manager System Guide* for details about user information.

- To add users individually from Cisco Unified Communications Manager Administration for Release 4.x, choose **User** > **Add a New User**.

  See "Adding a New User" chapter in *Cisco Unified Communications Manager Administration Guide* for more information about adding users. See *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, see *Bulk Administration Tool User Guide* (Cisco Unified Communications Manager Release 4.3 or later) or *Cisco Unified Communications Manager Bulk Administration Guide* (Cisco Unified Communications Manager Release 5.0 or later).

Related Topics

User Options Web Pages Management

From the User Options web page, users can customize and control several phone features and settings. For detailed information about the User Options web pages, see *Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G User Guide*.

Set up user access to 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 and associate appropriate phones with the user.

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 Product-specific fields for Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G, on page 163.

To set up user access, do the following.

Procedure

Step 1 For Cisco Unified Communications Manager Administration for release 5.x and later:
   a) From **User Management** > **User Group**, choose **User Management** > **End User**.
   b) Add the username.
   c) Add the phone.
   d) Associate the phone to the user.
   e) Add the user to a user group.

Step 2 For Cisco Unified Communications Manager Administration for Release 4.x, see *Cisco Unified Communications Manager Administration Guide*, "End User Configuration" section.

Customize User Options web page display

Most options that are on the User Options web pages appear by default. However, you must set the following options 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.

Custom Phone Rings Creation

You can customize the phone ring types available at your site by using a set of phone ring sounds provided by Cisco Unified Communications Manager or by creating your own pulse code modulation (PCM) files and editing the RingList.xml file. See the "Custom Phone Rings" chapter in the *Cisco Unified Communications Manager Features and Services Guide* for more information about customized ringtones.

Related Topics

C H A P T E R **8**

Security, Device, Model, Status, and Call Statistics Information

This chapter describes how to use the Settings menus on the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G to view the Security Configuration menu, Device Information menu, Model Information menu, Status menu, and the Call Statistics screen.

This chapter contains the following sections:

Display Security Configuration screen

To view the Security Configuration screen on the Cisco Unified Wireless IP Phone and see information about the security settings, follow these steps.

Procedure

Step 1 Choose **SETTINGS** > **System Configuration** > **Security**.

Step 2 Use the Navigation button to scroll through the items on the Security Configuration screen. Security Configuration fields, on page 176 describes the items that appear on this screen.

Step 3 To exit the Security Configuration screen, press the **Back** softkey.

Security Configuration fields

Table 36: Security Configuration fields

Field	Description
Web Access	Indicates web access capability for the phone. **Disabled** No user options web page access. **ReadOnly** Can view information. **Full** Can use configuration pages. You configure web access in Cisco Unified Communications Manager Administration.
Security Mode	Displays the security mode that is set for the phone. You configure the device security mode in Cisco Unified Communications Manager Administration. **Note** If you choose PEAP as your security mode, you can enable the validation of the server certificate on the phone.
MIC	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, see the "Using the Certificate Authority Proxy Function" chapter in *Cisco Unified Communications Manager Security Guide*.
LSC	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, see the "Using the Certificate Authority Proxy Function" chapter in *Cisco Unified Communications Manager Security Guide*.
CTL File	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, see the "Configuring the Cisco CTL Client" chapter in *Cisco Unified Communications Manager Security Guide***.** If a CTL file is installed on the phone, provides access to the CTL File screen. For more information, see CTL File Screen, on page 177.

Field	Description
Trust List	If a CTL file is installed on the phone, provides access to the Trust List screen. For more information, see Trust List Screen, on page 178.
CAPF Server	Displays the IP address or host name and the port of the CAPF that the phone uses.

CTL File Screen

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, see *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 server (TFTP Server 1) 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 DHCP Settings, on page 123.

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. For more information, see Security Profiles, on page 17.

Lock and unlock CTL file

To lock and unlock the CTL file, follow these steps:

Procedure

Step 1 If a CTL file is installed on the phone, choose **Settings** > **System Configuration** > **Security** > **CTL File**.

Step 2 Scroll to the CTL File menu and press **Select**.

Step 3 Press ****#** to unlock options on the CTL File menu.

Step 4 If you decide not to continue, press ****#** again to lock options on this menu.

Step 5 Scroll to the CTL option that you want to change and press **Erase**.
After you make the change, the CTL file locks automatically.

Step 6 To exit the CTL File screen, press **Exit** .

Trust List Screen

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

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.

Access Trust List screen

To access the Trust List screen on a phone with a CTL file,

Procedure

Step 1   Choosing **Settings** > **Security Configuration** > **Trust List**.

Step 2   To exit the Trust List screen, press the **Exit** softkey.

Related Topics

Device Information

You can access the Device Information screen on the Cisco Unified Wireless IP Phone 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

Related Topics

View Device Information screen

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 on the Device Information screen and press **Select**. The list of items under the category displays.

Device Information fields, on page 180 describes the categories and items that appear on this screen.

Step 3 To exit the Device Information screen, press **Back**.

Device Information fields

Table 37: Device Information categories and items

Item	Description
CallManager	
CallManager1 CallManager2 CallManager3 CallManager4 CallManager5	Hostnames 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. Each available server displays the Cisco Unified Communications Manager server IP address and one of the following states: **Active** Cisco Unified Communications Manager server from which the phone is currently receiving call-processing services. **Standby** Cisco Unified Communications Manager server to which the phone switches if the current server becomes unavailable. **Blank** No current connection to this Cisco Unified Communications Manager server.
Network	
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.

Item	Description
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.
WLAN	
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.
Scan Mode	Indicates when the phone scans. Configured in the Cisco Unified Communications Manager Administration.
Restricted Data Rates	Indicates the Traffic Stream Rate Set (TSRS) information element from CCX 1, which can define a data range for the client to use.
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.
Validate Server Certificate (Available when Security Mode is PEAP)	Indicates if the phone validates the RADIUS server during authentication. Requires a server certificate to be installed.
Encryption Type	Encryption method that the phone is currently using in the wireless network.

Item	Description
Key Management	Encryption key management that the phone is currently using in the wireless network.
Tx Power	Transmit power setting for the phone.
HTTP	
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	URL of proxy server, which makes HTTP requests to remote host addresses on behalf of the phone HTTP client and provides responses from the remote host to the phone HTTP client.
Idle URL	URL of an XML service that the phone displays when the phone has not been used for the time specified in the Idle URL Time option and no menu is open. For example, you could use the Idle URL option and the Idle URL Time option to display a stock quote or a calendar on the LCD screen when the phone has not been used for 5 minutes.
Idle URL Time	Number of seconds that the phone has not been used and no menu is open before the XML service specified in the Idle URL option is activated.
Locale	
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	
GARP Enabled	Indicates whether the phone learns MAC addresses from Gratuitous ARP responses.

Item	Description
Security Mode	Security mode assigned to the phone.
Web Access	Indicates web access capability for the phone. **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	
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.
UI	
BLF for Call Lists	Indicates whether the Busy Lamp Field (BLF) is enabled for call lists.
Reverting Focus Priority	Indicates whether the phone shifts the call focus on the phone screen to an incoming call or a reverting hold call.
Personalization	Indicates whether the phone has been enabled for configuration of custom ring tones and wallpaper images.

View Model Information screen

You can view the Model Information screen on the Cisco Unified Wireless IP Phone 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 on the Model Information screen.
Model Information fields, on page 184 describes the items that appear on this screen.

Step 3 To exit the Model Information screen, press **Back**.

Model Information fields

Table 38: Model Information fields

Field	Description
Model Number	Model number of the phone.
MAC Address	MAC address of the phone.
App Load ID	Identifier of the current firmware version running on the phone.
Serial Number	Serial number of the phone.
WLAN Regulatory Domain	Identifier for the wireless regulatory domain in which this phone must operate. **1050** North America (Cisco Unified Wireless IP Phone 7925G only) **3051** Europe (ETSI) (Cisco Unified Wireless IP Phone 7925G only) **4157** Japan (Cisco Unified Wireless IP Phone 7925G only) **5252** World mode including Australia/New Zealand, Asia, and Pacific (Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G)
USB Vendor ID	Unique code that identifies the vendor as Cisco.
USB Product ID	Unique code that identifies the phone as a Cisco product.
RNDIS Device Address	Manufacturer-assigned unique MAC address for the USB Remote Network Driver Interface Specification (RNDIS) for the phone.

Field	Description
RNDIS Host Address	Manufacturer-assigned unique MAC address for the USB RNDIS for the host.

Related Topics

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.

Network Statistics

Displays the Network Statistics screen, which shows Ethernet traffic statistics.

Call Statistics

Displays the Call Statistics screen, which shows counters, statistics, and voice quality metrics.

Firmware Versions

Displays the Firmware Versions screen, which shows information about the firmware running on the phone.

Neighbor List

Displays the neighboring APs and information on currently connected APs.

Site Survey

Displays the wireless media across all channels and locates APs that belong to the Basic Service Set (BSS).

Trace Settings

Displays the debug information for the phone. The following debug options are enabled from this screen:

- Remote syslog

- Trace levels

- Preserve logs

- Preserve trace levels

Related Topics

View Status Messages screen

You can use the Settings menu and Status menu to view status messages for the Cisco Unified Wireless IP Phone. 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. Network Statistics fields, on page 189 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:

Procedure

Step 1	Choose **Settings** > **Status**.
Step 2	Select **Status Messages**. The list of the status messages displays.
Step 3	To erase the messages, press **Clear**.
Step 4	To exit the screen, press **Back**.

Status messages

Table 39: Status messages, description, 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 corrupted.	For information about how to manage the MIC for your phone, see the "Using the Certificate Authority Proxy Function" chapter in *Cisco Unified Communications Manager Security Guide*.

Status message	Description	Possible explanation and action
CFG file not found	Neither the name-based configuration file nor default configuration file were not found on the TFTP Server.	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 CFG File Not Found response. • Phone is not registered with Cisco Unified Communications Manager. You must manually add the phone to Cisco Unified Communications Manager if you are not allowing phones to autoregister. See Cisco Unified Communications Manager phone addition methods, on page 50 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 IP Network Settings, on page 94 for details on assigning a TFTP server.
CTL Installed	A certificate trust list (CTL) file is installed in the phone.	None. This message is informational only. For more information about the CTL file, see *Cisco Unified Communications Manager Security Guide*.
CTL update failed	The phone could not update its certificate trust list (CTL) file.	Problem with the CTL file on the TFTP server. For more information, see *Cisco Unified Communications Manager Security Guide*.
Duplicate IP	Another device is using the IP address assigned to the phone.	• If the phone has a static IP address, verify that you have not assigned a duplicate IP address. See IP Network Settings, on page 94 section for details. • If you are using DHCP, check the DHCP server configuration.
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, see the "Using the Certificate Authority Proxy Function" chapter in *Cisco Unified Communications Manager Security Guide*.
LCS operation complete	The LCS was updated successfully on the phone.	For information about how to manage the LSC for your phone, see the "Using the Certificate Authority Proxy Function" chapter in *Cisco Unified Communications Manager Security Guide*.
TFTP Error	The phone does not recognize an error code provided by the TFTP server.	Contact the Cisco TAC.

Status message	Description	Possible explanation and action
TFTP server not authorized	The specified TFTP server could not be found in the phone CTL.	• 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.	• 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.

View configuration file name

You can use the Settings menu and Status menu to determine the name of the configuration file for the Cisco Unified Wireless IP Phone.

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:

SEP*macaddress*.cnf.xml or SEP*macaddress*.cnf.xml.enc.sgn.

Step 3 To exit the screen, press **Back**.

Related Topics

View 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 **SETTINGS** > **Status** > **Network Statistics**.
The list of statistics displays.

Step 2 Use the **Navigation** button to scroll through the items on the Network Statistics screen.
Network Statistics fields, on page 189 describes the items that appear on this screen.

Step 3 To exit the Network Statistics screen, press **Back**.

Related Topics

Network Statistics fields

Table 40: Network Statistics screen fields

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
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
RcvBeacons	Number of beacons received by the phone
AssocRej	Number of AP association rejections

Item	Description
AssocTmOut	Number of AP association timeouts
AuthRej	Number of authentication rejections
AuthTmOut	Number of authentication timeouts
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 acknowledgments 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
NullRcv	Number of null packets received
DataRcvBE	Number data packets received - Best Effort
DataRcvBK	Number data packets received - Background
DataRcvVI	Number data packets received - Video
DataRcvVO	Number data packets received - Voice

Call Statistics

You can access the Call Statistics screen on the phone to display counters, statistics, and voice quality metrics in these ways:

During the 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 using a web browser to access the Streaming Statistics web page. For more information about remote monitoring, see Remote Monitoring, on page 195

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.

Related Topics

View Call Statistics screen

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 on the Call Statistics screen.
Call Statistics fields, on page 192 describes the items that appear on this screen.

Step 4   To exit the Call Statistics screen, press **Back**.

Call Statistics fields

Table 41: Call Statistics fields

Field	Description
Rcvr Codec	Type of voice stream received (RTP streaming audio): G.729, G.722/iLBC, G.711 u-law, G.711 A-law, or Lin16k.
Sender Codec	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.
Sender Packets	Number of RTP voice packets transmitted since voice stream was opened. **Note** This number may not be 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). • Value1 is the average jitter in milliseconds (ms). • Value2 is the current audio frame buffer depth in m).
Max Jitter	Maximum jitter observed since the receiving voice stream was opened.
Rcvr Discarded	Number of RTP packets in the receiving voice stream that have been discarded (bad packets, too late, and so on). **Note** The phone discards payload type 19 comfort noise packets that are generated by Cisco Gateways, which increment this counter.
Rcvr Lost Packets	Missing RTP packets (lost in transit).
Voice Quality Metrics	

Field	Description
MOS LQK	Score that is an objective estimate of the mean opinion score (MOS) for listening quality (LQK) that rates from 5 (excellent) to 1 (bad). This score is based on audible concealment events due to frame loss in the preceding 8-second interval of the voice stream. For more information, see Voice Quality Monitoring, on page 221. **Note** The MOS LQK score can vary based on the type of codec that the Cisco Unified IP Phone uses.
Avg MOS LQK	Average MOS LQK score observed for the entire voice stream.
Min MOS LQK	Lowest MOS LQK score observed from start of the voice stream.
Max MOS LQK	Baseline or highest MOS LQK score observed from start of the voice stream. These codecs provide the following maximum MOS LQK score under normal conditions with no frame loss: • G.711 gives 4.5 • G.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.
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.
DSCP	Information about outbound and inbound previous and current frames.

Firmware Versions

You can verify the firmware versions that are used on the Cisco Unified Wireless IP Phone by viewing the Firmware Info screen. The firmware version name is in this format:

Product_Name-Model-Protocol.Version Number.Filetype

An example of a firmware release for the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G is cmterm-7925-sccp.X-0-0.cop.sgn.

Related Topics

View Firmware Versions screen

To display the firmware information, follow these steps:

Procedure

Step 1	Choose **SETTINGS** > **Status**.
Step 2	Select **Firmware Versions**.
Step 3	To view one of the items, scroll to the item and press **Select**.
Step 4	To exit the Firmware Versions screen, press **Back**.

Firmware Version fields

Table 42: Firmware Version fields

Item	Description
App Load ID	Identifies the phone firmware version running in the phone
Boot Load ID	Identifies the currently-installed boot load version 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

C H A P T E R **9**

Remote Monitoring

This chapter describes the methods for monitoring the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G using a web page.

Access web page for phone

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

Procedure

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

- Search for the phone in Cisco Unified Communications Manager by choosing **Devices** > **Phones**. Phones that are 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, press **SETTINGS** > **Device Information** > **Network** and then scroll to the IP Address option.

Step 2 Open a web browser and enter the following URL:
https://*<IP_address>*

where *IP_address* is the IP address of the Cisco Unified Wireless IP Phone

Note

Step 3 If the Security Alert dialog box displays a notice to accept the Trust Certificate, click **Yes** or **Always** to accept the application.

Step 4 Log in to the web pages with username admin and enter the password Cisco for the phone web pages.

Cisco Unified IP Phone Web Page Information

The web pages for a Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G includes these items for monitoring the phone:

- Wireless LAN Statistics: Provides information about the wireless LAN configuration.

- Network Statistics: Provides information about network traffic.

- Stream Statistics: Provides information about voice quality items.

Related Topics

Summary Information area

The Summary Information area on the phone web page displays network configuration information and information about other phone settings. The following table describes these items.

To display the Summary Information page, access the web page for the phone as described in the , and the Home: Summary page displays.

Table 43: 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	

Item	Description
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 Setup information

The Network Setup area on the phone's web page displays network configuration information and information about other phone settings. The following table describes these items.

To display the Network Information page, access the web page for the phone as described in the Access web page for phone, on page 195, and then click the **Network** hyperlink under the Information section.

Table 44: 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.

Item	Description
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.
Communications Manager Information	
CallManager 1–5	Host names or IP addresses, in prioritized order, of the Cisco Unified Communications Manager servers with which the phone can register. An item can also show the IP address of an SRST router that can provide limited Cisco Unified Communications Manager functionality, if such a router is available. Each available server shows the Cisco Unified Communications Manager server IP address and one of the following states: **Active** Cisco Unified Communications Manager server from which the phone is currently receiving call-processing services. **Standby** Cisco Unified Communications Manager server to which the phone switches if the current server becomes unavailable. **Blank** No current connection to this Cisco Unified Communications Manager server.
SRST Information	
SRST Reference IP	The IP Address for the Survivable Remote Site Telephony (SRST) designation, which identifies an SRST router able to provide Cisco Unified Communications Manager functionality with a limited feature set. This router assumes control of call processing if all other Cisco Unified Communications Manager servers become unreachable. The SRST Cisco Unified Communications Manager always appears last in the list of servers, even if it is active. 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.

Item	Description
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 reregisters 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

Item	Description
URL Information	
Information URL	URL of the help text that appears on the phone.
Directories URL	URL of the server from which the phone obtains directory information.
Messages URL	URL of the server from which the phone obtains message services.
Services URL	URL of the server from which the phone obtains Cisco Unified IP Phone services.
Idle URL	URL of an XML service that the phone displays when the phone has not been used for the time specified in the Idle URL Time option and no menu is open. For example, you could use the Idle URL option and the Idle URL Time option to display a stock quote or a calendar on the LCD screen when the phone has not been used for 5 minutes.
Idle URL Timer	Number of seconds that the phone has not been used and no menu is open before the XML service specified in the Idle URL option is activated.
Proxy Server URL	URL of proxy server, which makes HTTP requests to remote host addresses on behalf of the phone HTTP client and provides responses from the remote host to the phone HTTP client.
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 web page

The Device Information web page displays device settings and related information for the phone. The following table describes these items.

To display the Device Information area, access the web page for the phone as described in the Access web page for phone, on page 195, and then click the **Device** hyperlink under the information area.

Table 45: 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
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: **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

Item	Description
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 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 section

The Wireless LAN Statistics section provides information about packets that have been received and transmitted by the phone. The following table describes the statistics.

Table 46: 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
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

Item	Description
Tx Statistics (Best Effort)	
Tx OK Frames	Number of frames transmitted 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 acknowledgments 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 acknowlededements
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 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 acknowledgments by the AP
Retries Counter	Number of frames that were retransmitted

Item	Description
Multiple Retries Counter	Number of frames for which retransmission was attempted
Failed Retries Counter	Number of frames without acknowledgments
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

Network Statistics section

The Network Statistics section provides information about network traffic. The following table describes the IP, TCP, and UDP traffic.

Table 47: 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

Item	Description
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
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

Item	Description
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 menu

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. The following table describes each field displayed in the Stream Statistics window.

Table 48: Stream Statistics

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	Hostname for the phone

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.
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. **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 Topics

Troubleshooting

This chapter provides information that can assist you in troubleshooting your Cisco Unified Wireless IP Phone.

For additional troubleshooting information, see the *Cisco Unified Communications Manager Troubleshooting Guide*.

- Startup and Connectivity Problems, page 209
- Cisco Unified Wireless IP Phone Resets Unexpectedly, page 215
- Audio Problems, page 217
- Roaming and Voice Quality or Lost Connection Problems, page 219
- Voice Quality Monitoring, page 221
- Common Phone Status Messages, page 223
- General Troubleshooting Information, page 225
- Reset phone to factory defaults, page 228
- Troubleshooting Procedures, page 228

Startup and Connectivity Problems

After installing a Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G in your network and adding it to Cisco Unified Communications Manager Administration, the phone should start up as described in the Phone startup process, on page 66. If the phone does not start up properly, see the following sections for troubleshooting information.

Incomplete startup process

Problem

The phone does not start up and information does not display on the phone.

Cause

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.

Solution

To determine whether the phone is functional, follow these suggestions to systematically eliminate 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 to verify that the access point is active.

- Power on the Cisco Unified 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 the message `Low Battery` appears 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** button.

- The phone goes into recovery mode and checks the integrity of the firmware files.

- If an error message appears indicating `recovery required`, then plug the USB cable into the phone and a PC. See Set up USB LAN on PC, on page 70.

- Using a browser, access the web page for the phone. See Access phone web page, on page 71 for instructions.

- Go to the Phone Recovery section on the web page and upload a new Phone Software TAR file.

If, after you attempt these solutions, the phone still does not start up, contact a Cisco technical support representative for additional assistance.

No association to Cisco Aironet Access Points

After power on, 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.

The Cisco Unified Wireless IP Phone 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 (using the configured security mode setting)

4   Obtains an IP address

The following sections describe AP troubleshooting.

Access point settings mismatch

Problem

A configuration mismatch exists between the phone and the AP.

Solution

- Check the SSID settings on the access point and on the phone to be sure the SSIDs match.

- Check the authentication type settings on the access point and on the phone to be sure authentication and encryption settings match.

> **Note**   If the `No Service - IP Config Failed` message displays, 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 even if the WEP keys are incorrect or mismatched.

Authentication failed, No AP found

Problem

Authentication returns the `No AP found` message.

Solution

- Check whether 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, PEAP, or Auto (AKM) authentication.

- If you are using a WPA Pre-shared key or WPA2 Pre-shared Key, check that you have the correct passphrase configured.

- You might need to enter the username on the phone in the domain\username format when authenticating with a Windows domain.

EAP Authentication Failed message

Problem

Authentication returns the `EAP authentication failed` message.

Solution

- If you are using EAP, you might need to enter the EAP username 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

Problem

Authentication returned the `AP Error - Cannot support all requested capabilities` message.

Solution

On the access point, check that CKIP/CMIC is not enabled for the voice VLAN SSID. The Cisco Unified Wireless IP Phone does not support these features.

Phone Does Not Register with 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.

The following sections can assist you in determining the reason that the phone is unable to start up properly.

Cisco Unified Communications Manager phone Registration Rejected

Problem

The error message `Registration Rejected` displays.

Cause

A Cisco Unified Wireless IP Phone can register with a Cisco Unified Communications Manager server only if the phone has been added to the server or if autoregistration is enabled.

Solution

Review the information and procedures in Add Users to Cisco Unified Communications Manager, on page 172 to ensure that the phone has been added to the Cisco Unified Communications Manager database. Verify that the phone is in the Cisco Unified Communications Manager database, using **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 Device Information, on page 179.

If the phone is already entered in the Cisco Unified Communications Manager database, its configuration file may be damaged. See Configuration file corruption, on page 215 for assistance.

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

Problem

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

Solution

Ensure that the network is currently running.

TFTP server settings

Problem

The TFTP server setting on the phone is incorrect.

Cause

The Cisco Unified Wireless IP Phone 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 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.

Solution

If you have assigned a static IP address to the phone, you must manually enter this setting. See IP Network Settings, on page 94.

If you are using DHCP, the phone obtains the address for the TFTP server from the DHCP server. Check the IP address configured in the DHCP server.

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 IP Network Settings, on page 94 or View configuration file name, on page 188.

IP addressing and routing

Problem

The IP addressing and routing fields may not be correctly configured.

Solution

Verify the IP addressing for the Cisco Unified Wireless IP Phone. If you are using DHCP, the DHCP server should provide these values. If you have assigned a static IP address to the phone, you must enter these values manually.

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 timeout 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. See *Troubleshooting Switch Port Problems*, available at this URL: http://www.cisco.com/en/US/products/hw/switches/ps708/products_tech_note09186a008015bfd6.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 IP Network Settings, on page 94.

If you are using DHCP, check the IP addresses distributed by your DHCP server. Be aware of DHCP conflicts and duplicate IP addresses. See *Understanding and Troubleshooting DHCP in Catalyst Switch or Enterprise Networks*, available at this URL: http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a00800f0804.shtml.

For information about determining and changing IP addressing, see IP Network Settings, on page 94 .

DNS settings

Problem

The phone has incorrect DNS server information.

Solution

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 IP Network Settings, on page 94.

Cisco Unified Communications Manager and TFTP service status

Problem

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.

Cause

The Cisco Unified Wireless IP Phone attempts to open a TCP connection to all the Cisco Unified Communications Manager servers that are part of the assigned Cisco Unified Communications Manager group.

Solution

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.

For more information, see the *Cisco Unified Communications Manager Administration Guide* and the *Cisco Unified Serviceability Administration Guide*.

Configuration file corruption

Problem

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

Solution

Create a new phone configuration file. See Create new configuration file, on page 228.

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 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. The following sections can help you identify the cause of a phone resetting in your network.

Access point setup

Problem

The AP may not be configured correctly.

Solution

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 Site Survey Verification, on page 45 for information about access point settings.

Intermittent network outages

Problem

Your network may be experiencing intermittent outages.

Solution

Intermittent network outages affect data and voice traffic differently. Your network might be experiencing intermittent outages without detection. If so, data traffic can resend lost packets and verify that packets are received and transmitted. However, voice traffic cannot recapture lost packets. Rather than retransmitting a lost network connection, the phone resets and attempts to reconnect to the network. Contact the system administrator for information on known problems in the voice network.

DHCP settings errors

Problem

The DHCP settings may be incorrect.

Solution

Try the following actions:

- Verify that you have properly configured the phone to use DHCP. See Verify DHCP setup, on page 229.

- Verify that the DHCP server is set up properly.

- Verify the DHCP lease duration. Cisco recommends that you set the lease duration to 8 days.

Voice VLAN setup errors

Problem

If the Cisco Unified Wireless 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.

Solution

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 for details.

Phones Have Not Been Intentionally Reset

Problem

If you are not the only administrator with access to Cisco Unified Communications Manager, you should verify that no one else has intentionally reset the phones.

Solution

You can check if a Cisco Unified IP Phone received a command from Cisco Unified Communications Manager to reset by pressing **Applications** on the phone and choosing **Administrator Settings** > **Status** > **Network Statistics**.

- If the Restart Cause field displays `Reset-Reset`, the phone receives a Reset/Reset from Cisco Unified Communications Manager Administration.

- If the Restart Cause field displays `Reset-Restart`, the phone closed because it received a Reset/Restart from Cisco Unified Communications Manager Administration.

DNS or other connectivity errors

Problem

The phone reset continues and you suspect DNS or other connectivity issues.

Solution

If the phone continues to reset, eliminate DNS or other connectivity errors. See .

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, use the information in this section to identify the cause of the problem.

The following sections can assist you with audio problem troubleshooting.

Related Topics

One-way audio or no speech path

Problem

One or more people on a call do not hear any audio.

Solution

Use the following list to identify possible causes for the problem:

- Check the access point to see if 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 than that of the phone.

  Cisco Unified Wireless IP Phone 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 is in power save mode or scanning, the access point can respond to the wireless IP phone only when ARP caching is enabled.

  See Site Survey Verification, on page 45 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.

- Check that the speaker is functioning properly. Adjust the speaker volume setting and call the phone to check the speaker.

Ring volume is too low

Problem

User complains that the ringer on the phone is not loud enough.

Solution

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.

You can also press the **Volume** button on the side of the phone and the volume setting appears on the phone screen.

Phone does not ring

Problem

User complains that phone does not ring.

Solution

Check the phone settings:

- To see if the phone is set to ring, choose **Settings** > **Phone Settings** > **Sound Settings** > **Alert Pattern**, and check that a ring setting is selected.

- To see if a ringtone has been set for the phone, choose **Settings** > **Phone Settings** > **Ring Tone**. If none is set, add a ringtone for the phone.

- 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.

Roaming and Voice Quality or Lost Connection Problems

If users report that when they are engaged in an active phone call and walking from one location to another (roaming), the voice quality deteriorates or the connection is lost, use the information in this section to identify the cause of the problem.

The following sections can assist you with roaming issues.

Related Topics

Voice quality deteriorates while roaming

Problem

User complains that the voice quality deteriorates while roaming.

Solution

- 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.

Voice conversation delays while roaming

Problem

User complains of delays in the voice conversation while roaming.

Solution

- Use the Site Survey Utility on the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G to see if there is another acceptable access point as a roaming option. The next access point should have an signal of -67 dBm to roam successfully.

- Check the Cisco Catalyst 45xx switch. 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, 7925G-EX, and 7926G (or any wireless client) experiences roaming delays when an earlier version (SUP 1 or SUP2) blade is used.

PhonelosesCiscoUnifiedCommunicationsManagerconnectionwhileroaming

Problem

User complains that the call gets dropped while roaming.

Solution

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 is capable of Layer 2 roaming only. Layer 3 roaming requires WLSM that uses GRE. For more information, see WLANs and roaming, on page 30.

- If using EAP-FAST, LEAP, or Auto (AKM) authentication, the access point might be using filters to block TCP ports. The RADIUS server uses port 1812 for authentication and 1813 for accounting.

Phone does not roam back to preferred band

Problem

The phone does not roam back to the preferred wireless band.

Solution

For troubleshooting information, see the *Cisco Unified Wireless IP Phone 7925 and 7926 Series Deployment Guide*.

Voice Quality Monitoring

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

Concealment Ratio metrics

Shows the ratio of concealment frames over total speech frames. An interval conceal ratio is calculated every 3 seconds.

Concealed Second metrics

Shows the number of seconds in which the DSP plays concealment frames due to lost frames. A severely "concealed second" is a second in which the DSP plays more than 5 percent concealment frames.

MOS-LQK metrics

Uses a numeric score to estimate the relative voice listening quality. The Cisco Unified IP Phone calculates the mean opinion score (MOS) for listening quality (LQK) based audible concealment events due to frame loss in the preceding 8 seconds, and includes perceptual weighting factors such as codec type and frame size.

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, see 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 .

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 MOS LQK scores under normal conditions with zero frame loss:

- G.711 and G.722 codecs have maximum scores of 4.5

- G.729A/AB codec has a maximum score of 3.8

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

Voice quality troubleshooting tips

When you observe significant and persistent changes to metrics, use the following table for general troubleshooting information.

Table 49: Changes to voice quality metrics

Metric change	Condition
MOS LQK scores decrease significantly	Network impairment from packet loss or high jitter: - Average MOS LQK decreases could indicate widespread and uniform impairment. - Individual MOS LQK decreases indicate bursty impairment. Cross-check with Conceal Ratio and Conceal Seconds for evidence of packet loss and jitter.
MOS LQK scores decrease significantly	- Check to see if the phone is using a different codec than expected (Sender Codec and Rcvr Codec). - Check to see if the MOS LQK version changed after a firmware upgrade.
Conceal Ratio and Conceal Seconds increase significantly	- Network impairment from packet loss or high jitter.

Metric change	Condition
Conceal Ratio is near or at zero, but the voice quality is poor	• 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, hands-free cellular phone or wireless headset. Check packet transmit (TxCnt) and packet receive (RxCnt) counters to verify that voice packets are flowing.

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

Common Phone Status Messages

The following sections describe the common status messages that display on the phone screen.

Network Busy message

Problem

The phone is unable to complete a call. The phone displays the `Network Busy` message.

Cause

The WLAN is not able to allocate bandwidth for the phone to complete the call.

Solution

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 message

Problem

The phone is unable to place or receive calls. The no signal icon displays on the phone screen. The phone displays the `Leaving Service Area` message.

Cause

The phone cannot detect any access point (AP) beacons

Solution

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 message

Problem

The phone is searching for an AP and the phone displays the `Locating Network Services` message.

Cause

The phone is searching all beacons and scanning for a channel and SSID to use.

Solution

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 message

Problem

The phone is unable to access the WLAN, and the main phone screen is not active. The phone displays the `Authentication Failed` message.

Cause

The authentication server does not accept the security credentials.

Solution

Verify that the security mode and credentials are correct by viewing the Network profile. For information about accessing and changing Network profiles, see Access Network Profile menu, on page 119.

Configuring IP message

Problem

The main phone screen is not active and the phone displays the `Configuring IP` message.

Cause

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.

Solution

Wait a few minutes for the phone to obtain the network parameters.

If the phone unable to retrieve the IP address, check that the DHCP server is up and running.

Configuring CM List message

Problem

The main phone screen is not active and the phone displays the `Configuring CM List` message.

Cause

The phone is downloading its configuration files from the TFTP server.

Solution

Wait a few minutes for the phone to download all of its configuration files.

General Troubleshooting Information

The following table provides general troubleshooting information for the wireless IP phone.

Table 50: Cisco Unified Wireless IP Phone Troubleshooting Tips

Summary	Explanation
Phone is resetting	The phone resets when it loses contact with the Cisco Unified Communications Manager software. This lost connection can be due to any network connectivity disruption, including access point problems, switch outages, and switch reboots. See Cisco Unified Wireless IP Phone Resets Unexpectedly, on page 215.
Time on phone is incorrect	Sometimes the time or date on the phone is incorrect. The Cisco Unified Wireless IP Phone gets its time and date when it registers with Cisco Unified Communications Manager. Power cycle the phone to reset the time or date. The time shows in either 12 hour or 24 hour format.
Phone firmware downgrades	After applying a Cisco Unified Communications Manager upgrade or patch, that is older than the current Cisco Unified Wireless IP Phon firmware, the phones could automatically downgrade to the load contained in the patch. Check the Cisco Unified Wireless IP Phone default image in the TFTP folder to fix this problem.

Summary	Explanation
Battery life is shorter than specified	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. Higher phone transmit power can affect battery life. 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.
Phone call cannot be established	The phone does not have a DHCP IP address, is unable to register to Cisco Unified Communications Manager, and shows a `Configuring IP` or `Registering` message. Verify the following: 1 The 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	Call statistics display does not show iLBC as the receiver/sender codec. 1 Check the following using the Cisco Unified Communications Manager administration pages: • 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

Log Information for Troubleshooting

The following sections can help you gather troubleshooting information.

Related Topics

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 are 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 Set up Trace Settings, on page 98.

Phone Trace Logs

When you are experiencing problems registering with Cisco Unified Communications Manager, or call connections, you can use the Trace Logs 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.

Related Topics

Prevent 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 Exit all Internet Explorer sessions.

Reset phone to factory defaults

You can clear all locally stored configuration options in a phone from 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   Perform one of the following actions:

- Press **Yes** to delete all settings. The phone cycles through normal startup procedures.

- 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

Troubleshooting Procedures

Use the procedures in this section to resolve problems.

Create new configuration file

Note   When you remove a phone from the Cisco Unified Communications Manager database, its configuration file is deleted from the Cisco Unified Communications Manager TFTP server. The 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. See *Cisco Unified Communications Manager Administration Guide* for more information.

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 that is not working properly.
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 Add Users to Cisco Unified Communications Manager, on page 172 for details.
Step 4	Power cycle the phone.

Related Topics

Verify DHCP setup

To determine if the phone has been properly configured to use DHCP, follow these steps.

Procedure

Step 1	Verify that you have properly configured the phone to use DHCP. See DHCP Settings, on page 123 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 is denied, forcing the phone to restart and request a new IP address from the DHCP server.

Determine DNS or connectivity issues

To eliminate DNS or other connectivity errors, follow these steps.

Procedure

Step 1	Reset the phone to factory defaults. See Reset phone to factory defaults, on page 228 for details.
Step 2	Modify DHCP and IP settings:
	a) Disable DHCP. See DHCP Settings, on page 123 for details.

b) Assign static IP values to the phone. See DHCP Settings, on page 123 for details. Use the same default router setting used for other functioning Cisco Unified IP Phones.

c) Assign a TFTP server. See Set alternate TFTP server, on page 124 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 hostname.

Note   Cisco recommends that you configure only IP addresses and not hostnames 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 Device Information, on page 179.

Step 5   Power cycle the phone.

APPENDIX **A**

Internal Support 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, 7925G-EX, and 7926G (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, 7925G-EX, and 7926G.

Consider adding the following types of information to this site:

Cisco Unified Wireless IP Phone Operations

Users need to know that their Cisco Unified Wireless IP Phone 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 are 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 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 wireless IP phone differs from the desktop IP phone as follows:

• No line buttons: You must enter the phone number from the keypad 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

Phone care and maintenance

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, 7925G-EX, and 7926G:

• Use only chargers, batteries, and accessories that are approved by the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G 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 or contaminants, and hard impacts can invalidate the one-year hardware warranty.

For a list of available accessories and their descriptions, see the *Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G Accessory Guide* at this URL:

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

Help System on Phone

This Cisco Unified Wireless IP Phone 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.

Cisco Unified Wireless IP Phone manuals

You should provide end users with access to user documentation for the Cisco Unified Wireless IP Phones. This documentation includes detailed user instructions for key phone features.

There are several Cisco Unified IP Phone models available, so to assist users in finding the appropriate documentation on the Cisco website, Cisco recommends that you provide links to the current documentation. If you do not want to or cannot send users to the Cisco website, Cisco suggests that you download the PDF files and provide them to end users on your website.

Related Topics

User 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).

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

User Voice Messaging System Access

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, see 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, see 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

See the *Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G User Guide* for information about accessing the voice messaging system from the phone.

International User Support

Translated and localized versions of the Cisco Unified IP Phones are available in several languages. If you are supporting Cisco Unified IP Phones in a non-English environment, see the following section to ensure that the phones are set up properly for your users.

Before you deploy 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

This section includes the following information:

- Cisco Unified Communications Manager Locale Installer Installation, page 235

Cisco Unified Communications Manager Locale Installer Installation

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 that are 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, see the "Locale Installation" section in the *Cisco Unified Communications Operating System Administration Guide*.

Note   All languages may not be immediately available, so continue to check the website for updates.

Technical Specifications

The following sections describe the technical specifications for the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G.

- Cisco Unified Wireless IP Phone 7925G and 7926G Physical and Operating Environment Specifications, page 237
- Cisco Unified Wireless IP Phone 7925G-EX physical and operating environment specifications, page 238

Cisco Unified Wireless IP Phone 7925G and 7926G Physical and Operating Environment Specifications

The following table shows the physical and operating environment specifications for the Cisco Unified Wireless IP Phone 7925G and 7926G.

Table 51: Cisco Unified Wireless IP Phone 7925G and 7926G 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% (noncondensing)
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 6500 ft (0 to 2 km)

Specification	Value or range
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) The weight depends on the weight of the battery pack.
LCD	2 inches wide with 176 by 220 pixel resolution
Power	AC adapters by geographic region

Cisco Unified Wireless IP Phone 7925G-EX physical and operating environment specifications

The following table shows the physical and operating environment specifications for the Cisco Wireless IP Phone 7925G-EX.

Table 52: Cisco Unified Wireless IP Phone 7925G-EX physical and operating environmental specifications

Specification	Value or range
Operating Temperature	-10 to 50°C (14° to 122°F)
Operating Relative Humidity	10% to 95% (noncondensing)
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 6500 ft (0 to 2 km)
Endurance	IP64; MIL-STD-810F, Method 516.5, Procedure I
Phone Height	5.0 in. (12.7 cm)

Specification	Value or range
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) The weight depends on the weight of the battery pack.
LCD	2 inches wide with 176 by 220 pixel resolution
Power	AC adapters by geographic region

Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G Deployment Overview

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

Wireless Network Setup

For information about WLAN configuration, see *Cisco Unified Wireless IP Phone 7925 and 7926 Series Deployment Guide* at http://www.cisco.com/en/US/products/hw/phones/ps379/products_implementation_design_guides_list.html.

QoS Policies Setup

For information about QoS policies, see *Cisco Unified Wireless IP Phone 7925 and 7926 Series Deployment Guide*.

Cisco Unified Communications Manager setup for Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G

The following steps provide an overview and checklist of configuration tasks for the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G in Cisco Unified Communications Manager Administration. The steps 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, see the sources in the steps.

Procedure

Step 1 Gather the following information about the phone:

- 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

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

For more information, see

- *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phone" chapter

- Telephony features available, on page 150

Step 2 Customize phone button templates (if required) to change the number of line buttons, speed-dial buttons, Service URL buttons, or to add a Privacy button to meet user needs.
For more information, see

- *Cisco Unified Communications Manager Administration Guide*, "Phone Button Template Configuration" chapter

- Phone Button Templates, on page 168

Step 3 Add and configure the phone by completing the required fields in the Phone Configuration window. Required fields are indicated by an asterisk (*) next to the field name; for example, MAC address and device pool. This step adds the device with its default settings to the Cisco Unified Communications Manager database.

For more information, see

- *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Configuration" chapter

- "?" Button Help in the Phone Configuration window

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

This step adds primary and secondary directory numbers and features associated with directory numbers to the phone.

For more information, see

- *Cisco Unified Communications Manager Administration Guide*, "Directory Number Configuration" chapter, "Creating a Cisco Unity Voice Mailbox" section

- Telephony features available, on page 150

Step 5 Customize softkey templates. This step adds, deletes, or changes the order of softkey features that display on the user's phone to meet feature use needs.
For more information, see

- *Cisco Unified Communications Manager Administration Guide*, "Softkey Template Configuration" chapter

- Softkey Templates, on page 166

Step 6 Assign line view speed-dial numbers. This step adds line view speed-dial numbers.
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.
Note Users can change line view speed-dial settings on their phones by using Cisco Unified CM User Options.
For more information, see

- *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Configuration" chapter, "Configuring Speed-Dial Buttons" section

- *Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G User Guide*, "Call Features" chapter, "Speed Dialing" section

- Telephony features available, on page 150

Step 7 Configure Cisco Unified IP Phone services and assign services (optional). This step provides IP Phone services.
Note Users can add or change services on their phones by using the Cisco Unified CM User Options.

For more information, see

- *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Services Configuration" chapter

- Services Menu, on page 168

Step 8 Add user information by configuring required fields. Required fields are indicated by an asterisk (*); for example, User ID and last name.
Note Assign a password (for User Options web pages) and PIN (for Extension Mobility and Personal Directory)
This step adds user information to the global directory for Cisco Unified Communications Manager.

For more information, see

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

- Add Users to Cisco Unified Communications Manager, on page 172

Step 9 Associate a user to a user group. This step assigns to 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.

Note Applicable to Cisco Unified Communications Manager Administration Release 5.x and later.

For more information, see the *Cisco Unified Communications Manager Administration Guide*:

- "End User Configuration" chapter, "End User Configuration settings" section

- "User Group Configuration" chapter, "Adding Users to a User Group" section

Step 10 Associate a user with a phone. This step is optional if you do not want users to have access to User Options. This step provides users with control over their phone such as forwarding calls or adding line view speed-dial numbers or services.

Note Some phones, such as those used by multiple users, do not have an associated user.

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

Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G installation

The following steps provide an overview and checklist of installation tasks for the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G. The steps 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, see the sources in the steps.

Procedure

Step 1 Assemble the phone components and charge the battery.
For more information, see Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G Installation, on page 20.

Step 2 Configure the network profile by using the USB cable and the phone web page.
For more information, see Access web page for phone, on page 195.

Step 3 Configure the phone settings by using the **Settings** menu on the phone.
For more information, see Phone Settings Menu, on page 129.

Step 4 Power on the phone and monitor the phone startup process.
For more information, see:

- Phone startup process, on page 66

- Startup and Connectivity Problems, on page 209

Step 5 Make calls with the wireless IP phone.

For more information, see:

- *Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G User Guide*

- Roaming and Voice Quality or Lost Connection Problems, on page 219

Step 6   Provide information to end users about how to use their phones and how to configure their phone options. For more information, see Internal Support Website, on page 231.

I N D E X