C H A P T E R 1

Overview of the Cisco Unified Wireless IP Phone 7925G

This chapter includes the following sections:

Understanding the Cisco Unified Wireless IP Phone 7925G

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

The Cisco Unified Wireless IP Phone 7925G is an 802.11 dual band wireless device that provides comprehensive voice communications in conjunction with Cisco Unified Communications Manager and Cisco Aironet 802.11b/g and Cisco Aironet 802.11a Access Points (APs) in a private business communications network. This phone model, like other network devices, must be configured and managed. This phone encodes G.711a, G.711u, G.729a, G.729ab, G.722/iLBC, and decodes G.711a, G711b, G.711u, G.729, G729a, G729b, and G729ab. The phone also supports uncompressed wideband (16 bits, 16 kHz) audio.

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

The physical characteristics include:

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

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

Bluetooth Technology

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

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

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

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

Bluetooth devices fit into to three different power classes, as shown in Table 1-1.

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

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

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

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

Handsfree Profile

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

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

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

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

    – End the active call and answer or resume a waiting call.

    – Put the active call on hold and answer or resume a waiting call.

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

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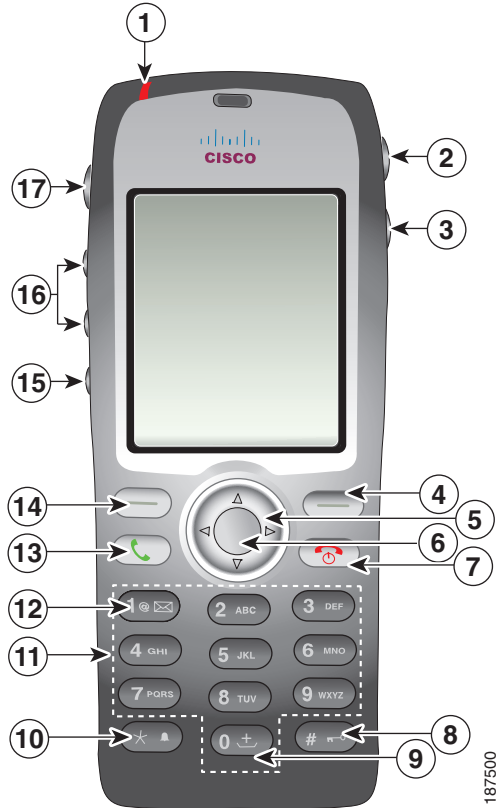
Pairing with Headsets

The Cisco Unified Wireless IP Phone 7925G pairs with headsets by using a shared key authentication/encryption method. This process requires confirmation of a PIN specific to the headset, commonly "0000." The Cisco Unified Wireless IP Phone 7925G can be paired with more than one headset at a time. Pairing is typically performed once for each headset used with the Cisco Unified Wireless IP Phone 7925G. Once pairing is complete, the headset automatically connects to the Cisco Unified Wireless IP Phone 7925G when both devices are powered on and in range.
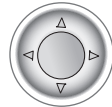
Note   The Cisco Unified Wireless IP Phone 7925G can only be connected to one Bluetooth-enabled headset at a time. Further, the Cisco Unified Wireless IP Phone 7925G only supports communication with Bluetooth wireless technology-enabled devices qualified by the Bluetooth Special Interest Group (SIG).

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

Figure 1-1   *Cisco Unified Wireless IP Phone 7925G*

1	Indicator light (LED)	Provides these indications:
		• Solid red—Phone is connected to AC power source and battery is charging.
		• Solid green—Phone is connected to AC power source and battery is fully charged.
		• Fast blinking red—Incoming call. (Phone can be charging or fully charged.)
		• Slow blinking red—Voice message. (When connected to AC power source, red light displays longer than when phone is using only the battery.)
		• Slow blinking green—Phone is using only battery power. Phone is registered with the wireless network and is within service coverage area.
2	Headset port cover	Cover for the headset port.
3	Speaker button	Toggles the speaker mode on or off for the phone.
4	Right softkey button	Activates the Options menu for access to the list of softkeys. Sometimes displays a softkey label.

5	Navigation button	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, silences a ringing call, or ends a connected call.
		When using menus, acts as a shortcut to return to the main screen.
8	Pound (#) key	Toggles between locking and unlocking the keypad.
		Allows you to enter these special characters when you are entering text: **# ? ( ) [ ] { }**
9	Zero (0) key	Enters "0" when dialing a number. Allows you to enter a space or these special characters when you are entering text: **+ , . ' " | _ ~ '**
		Note When entering text or dialing an international number, use the plus sign (+).
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.
		Press and hold key 1 to access your voice messaging system.
12	One (1) key	Enters "1" when dialing a number. Allows you to access the voice messaging system.
		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 customized by the phone administrator or user, allows direct access to the Phone Book or voice messages.
15	Mute button	Toggles the mute feature on or off.
16	Volume button	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.
17	Application button	Configurable button that is used with XML applications, such as Push to Talk or Directory services. See "Setting Up Services" section on page 7-17.

Related Topics

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

Features Supported on the Cisco Unified Wireless IP Phone 7925G

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

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

This section provides information about these topics:

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

Feature Overview

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

- Bluetooth Class 2 technology for headsets that support Bluetooth

- Six-line appearance

- Adjustable ring and volume levels

- Adjustable display brightness and time outs

- Auto-detection of headset and auto-answer from the headset

- Wireless web access to your phone number and the corporate directory

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

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

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

Related Topics

- Configuring Network Profiles, page 4-8

- Configuring Features, Templates, Services, and Users, page 7-1

Telephony Features

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

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

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

Related Topic

- Telephony Features Available for the Phone, page 7-2

Network Settings Configuration

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

- Cisco Unified Wireless IP Phone 7925G web pages

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

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

You can also configure network settings on the phone itself. For more information about configuring features from the phone, see Chapter 5, "Configuring Settings on the Cisco Unified Wireless IP Phone 7925G."

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

Related Topics

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

Feature Information for Users

If you are a system administrator, you are the primary source of information for Cisco Unified Wireless IP Phone users in your network or company. To ensure that you distribute the most current feature and procedural information, familiarize yourself with Cisco Unified Wireless IP Phone 7925G documentation. Make sure to visit the Cisco Unified IP Phone web site:

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

From this site, you can view additional phone documentation.

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

For a summary of the key information that you can provide to phone users, see Appendix A, "Providing Information to Users By Using a Website."

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

Related Topic

- Providing Information to Users By Using a Website, page A-1

Understanding Security Features for Cisco Unified IP Phones

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

For information about supported security options for the Cisco Unified Wireless IP Phone 7925G, see the "Authentication Methods" section on page 2-16.

For information about security features supported by Cisco Unified Communications Manager and Cisco Unified IP Phones, see the "Understanding Security Features for Cisco Unified IP Phones" section on page 1-8.

Table 1-2 provides additional information about security topics.

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

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

Overview of Supported Security Features

Table 1-3 provides an overview of the security features that the Cisco Unified Wireless IP Phone 7925G supports. For more information about these features and about Cisco Unified Communications Manager and Cisco Unified IP Phone security, refer to *Cisco Unified Communications Manager Security Guide*.

For information about current security settings on a phone, choose **SETTINGS > System Configuration > Security**. For more information, see the "Viewing Security Information" section on page 8-1.

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

Table 1-3   Description of Security Features

Feature	Description
Image authentication	Prevents tampering with the firmware image before it is loaded on a phone by using signed binary files (with the extension.sbn). Tampering with the image causes a phone to fail the authentication process and reject the new image.
Customer-site certificate installation	Authenticates each Cisco Unified IP Phone by using a unique certificate. Phones include a manufacturing installed certificate (MIC), but for additional security, you can specify in Cisco Unified Communications Manager Administration that a certificate be installed by using the Certificate Authority Proxy Function (CAPF). Alternatively, you can install a locally significant certificate (LSC) from the Security Configuration menu on the phone. See the "Configuring the Security Certificate on the Phone" section on page 5-12 for more information.
Device authentication	Occurs between the Cisco Unified Communications Manager server and the phone when each entity accepts the certificate of the other entity. Determines whether a secure connection between the phone and a Cisco Unified Communications Manager should occur, and, if necessary, creates a secure signaling path between the entities using TLS protocol. Cisco Unified Communications Manager will not register phones unless authenticated by the Cisco Unified Communications Manager.
File authentication	Validates digitally-signed files that the phone downloads. The phone validates the signature to make sure that file tampering did not occur after the file creation. Files that fail authentication are not written to Flash memory on the phone. The phone rejects such files without further processing.
Signaling Authentication	Uses the TLS protocol to validate that no tampering has occurred to signaling packets during transmission.

Table 1-3 **Description of Security Features (continued)**

Feature	Description
Manufacturing installed certificate	Each Cisco Unified IP Phone contains a unique manufacturing installed certificate (MIC), which is used for device authentication. The MIC is a permanent unique proof of identity for the phone, and allows Cisco Unified Communications Manager to authenticate the phone.
Secure Cisco Unified SRST reference	After you configure a SRST reference for security and then reset the dependent devices in Cisco Unified Communications Manager Administration, the TFTP server adds the SRST certificate to the phone cnf.xml file and sends the file to the phone. A secure phone then uses a TLS connection to interact with the SRST-enabled router.
Media encryption	Uses SRTP to ensure that the media streams between supported devices proves secure and that only the intended device receives and reads the data. Includes creating a media master key pair for the devices, delivering the keys to the devices, and securing the delivery of the keys while the keys are in transport.
Signaling encryption by using TLS	Ensures that all SCCP signaling messages that are sent between the device and the Cisco Unified Communications Manager server are encrypted.
CAPF (Certificate Authority Proxy Function)	Implements parts of the certificate generation procedure that are too processing-intensive for the phone, and it interacts with the phone for key generation and certificate installation. The CAPF can be configured to request certificates from customer-specified certificate authorities on behalf of the phone, or it can be configured to generate certificates locally.
Security profiles	Defines whether the phone is non-secure, authenticated, or encrypted. See the "Understanding Security Profiles" section on page 1-12 for more information.
Encrypted configuration files	Lets you ensure the privacy of phone configuration files.
Optional disabling of the web server functionality for a phone	You can prevent access to a phone web page, which displays a variety of operational statistics for the phone.
Phone hardening	Additional security options, which you control from Cisco Unified Communications Manager Administration: • 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 the "Viewing Security Information" section on page 8-1.

Related Topics

Understanding Security Profiles

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

> **Note** For Cisco Unified IP Phones using Cisco Unified CallManager 4.1 and later, security is configured on each phone. For more information about configuring security, refer to *Cisco Unified CallManager Security Guide* at
> http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.

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

Related Topics

Identifying Authenticated, Encrypted, and Protected Phone Calls

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

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

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

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

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

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

Establishing and Identifying Protected Calls

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

A protected call is established using this process:

1. A user initiates the call from a protected phone (protected security mode).

2. The phone displays the [icon] icon (encrypted) on the phone screen. This icon indicates that the phone is configured for secure (encrypted) calls, but this does not mean that the other connected phone is also protected.

3. A security tone plays if the call is connected to another protected phone, indicating that both ends of the conversation are encrypted and protected. If the call is connected to a non-protected phone, then the secure tone is not played.

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

Related Topics

- Understanding Security Features for Cisco Unified IP Phones, page 1-8
- Understanding Security Profiles, page 1-12
- Security Restrictions, page 1-13

Security Restrictions

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

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

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

A user can barge into an authenticated call, even if the phone that is used to barge is non-secure. The authentication icon continues to display on the authenticated phones in the call, even if the initiator's phone does not support security.

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

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

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

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

- Configuring the Cisco Unified Wireless IP Phone 7925G in Cisco Unified Communications Manager, page 1-14
- Installing the Cisco Unified Wireless IP Phone 7925G, page 1-15

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

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

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

For more information about these choices, see the "Methods for Adding Phones to Cisco Unified Communications Manager" section on page 3-2.

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

For a checklist of tasks for configuring the phone in Cisco Unified Communications Manager, see the "Configuring the Cisco Unified Wireless IP Phone 7925G in Cisco Unified Communications Manager" section on page D-4.

Related Topics

- Installing the Cisco Unified Wireless IP Phone 7925G, page 1-15

- Configuring Features, Templates, Services, and Users, page 7-1

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

Installing the Cisco Unified Wireless IP Phone 7925G

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

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

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

Note   Before you install a phone, even if it is new, upgrade the phone to the current firmware image. For information about upgrading, refer to the Readme file for your phone which is located at: http://www.cisco.com/cgi-bin/tablebuild.pl/ip-7900ser-crypto.

For a checklist of tasks for installing the phone, see the "Installing the Cisco Unified Wireless IP Phone 7925G" section on page D-7.

Related Topics

- Understanding the Cisco Unified Wireless IP Phone 7925G, page 1-1

- Overview of Configuring and Installing the Cisco Unified Wireless IP Phone 7925G, page 1-14

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

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