Cisco Wireless IP Phone 8821 and 8821-EX Administration Guide for Cisco Unified Communications Manager

First Published: 2016-06-29

Last Modified: 2019-12-13

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

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

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

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

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

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

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

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

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

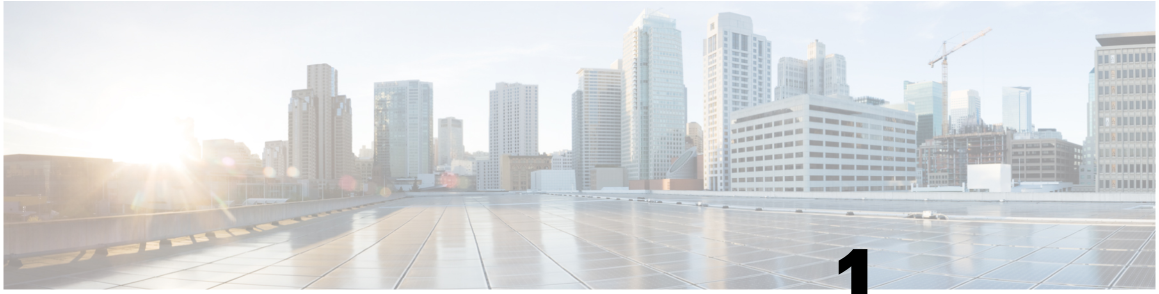
IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY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

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

CONTENTS



CHAPTER 1

Your Phone

Cisco Wireless IP Phone 8821 and 8821-EX

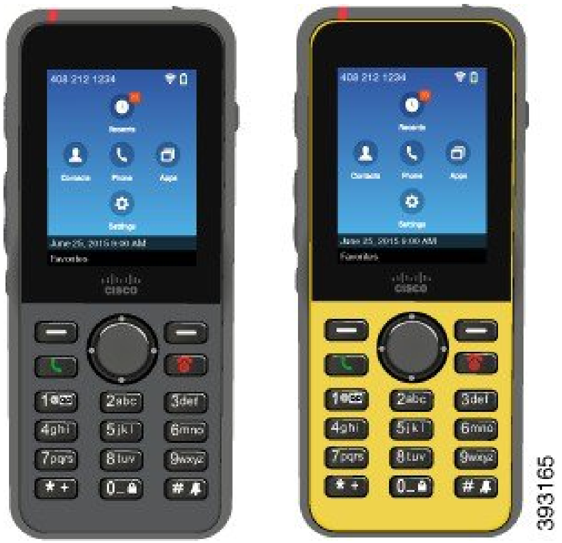
The Cisco Wireless IP Phone 8821 and 8821-EX are 802.11 dual-band wireless devices that provide comprehensive voice communications in conjunction with Cisco Unified Communications Manager and with Cisco Aironet and Cisco Meraki access points (APs) in a private business communications network.

The phones provide 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 Cisco Wireless IP Phone 8821-EX is certified for Potentially Explosive Atmosphere ATEX Zone 2 IP54 (pending) and North America Class I Division 2/Zone 2. The phone is certified for use in potentially explosive (hazardous) environments where flammable gases, vapors or liquids may be present for a short period of time or under abnormal conditions. The phone has an industry-standard yellow styling that offers fast recognition in emergency situations.

The following figure shows the Cisco Wireless IP Phone 8821 on the left and the Cisco Wireless IP Phone 8821-EX on the right.

Figure 1: Cisco Wireless IP Phone 8821 and 8821-EX



These phones, like other network devices, must be configured and managed. The phones support G.711a. G.711u, G.722, G.729a, G.729ab, iLBC, iSAC, and OPUS codecs. The phones also support uncompressed wideband (16 bits, 16 kHz) audio.

The phones are hearing aid compatible (HAC) but do not have any TTY features. They have ridges on the sides of 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
- Shockproof and vibration-proof
- USB On-the-Go (OTG) 2.0 interface
- Cisco Wireless IP Phone 8821: IP54 protection, which indicates dust-tight equipment that is protected against water (see below)
- Cisco Wireless IP Phone 8821-EX only:
    - IP67 protection in ordinary locations
    - Certified for use in Potentially Explosive Atmosphere:
        - ATEX Zone 2 IP54 (pending)
        - METLABS Certified for Class I and II, Division 2 and Class III, Divisions 1 and 2, Groups A, B, C and D
    - Industry-standard yellow styling offers fast recognition in emergency situations.
- Charge with a desktop charger for a single phone or a multicharger for up to 6 phones. For more information, see Supported Accessories, on page 103.

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
- Access to network data, XML applications, and web-based services
- Online customizing of phone features and services from your Self Care portal

To prevent device damage:

- Don't bathe or swim with the phone.
- Don't expose phone to pressurized water or high velocity water, such as when showering, cleaning, or hand washing.
- Don't use the phone in a sauna or steam room.
- Don't intentionally submerge phone in water.
- Don't operate the phone outside the suggested temperature ranges or in extremely humid, hot, or cold conditions.
- Don't store phones, batteries, and accessories outside the suggested temperature ranges or in extremely humid, hot, or cold conditions.
- Don't drop the phone or subject it to other impacts.
- Don't disassemble the phone; don't remove any screws.
- Don't use harsh cleaning agents, like bleach and other chemicals, to clean the phone exterior
- Don't use a broken battery door or a battery door with a broken seal.

Minimize the exposure of your phone to soap, detergent, acids or acidic foods, and any liquids; for example, salt water, soapy water, pool water, perfume, insect repellent, lotions, sun screen, oil, adhesive remover, hair dye, soft drinks, and solvents. For more information, see Care of Your Phone, on page 7.

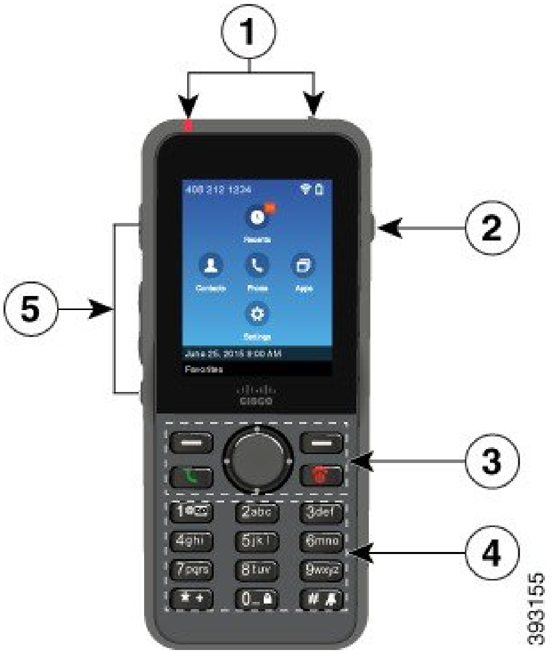
IP54 and IP67

The Cisco Wireless IP Phone 8821 and 8821-EX are tested under controlled laboratory conditions under IEC standard 60529. The Cisco Wireless IP Phone 8821 has a rating of IP54 and the Cisco Wireless IP Phone 8821-EX has a rating of IP67 in ordinary locations. Ingress Protection 54 (IP54) and Ingress Protection 67 (IP67) indicate dust-tight equipment that is protected against water. Splash, water, and dust resistance are not permanent conditions, and resistance might decrease as a result of normal wear. Users are expected to take care of the phone and should not deliberately expose the device to a hostile environment of dust, splash, or water immersion.

Buttons and Hardware

Your wireless phone has many buttons and hardware features that you will use regularly. Use the following figure and table to identify the important button and hardware features. The following figure shows the Cisco Wireless IP Phone 8821, but the Cisco Wireless IP Phone 8821-EX is similar in appearance.

Figure 2: Cisco Wireless IP Phone 8821 Buttons and Hardware



The following table describes the functions of the keys on the phones.

Item	Name or Grouping	Description
1	Indicator light (LED) Headset port	Indicator light—Use the light to identify states: • Solid red—the phone is connected to the AC power source and battery is charging. • Solid green—the phone is connected to the AC power source and battery is fully charged. • Fast blinking amber—There is an incoming call. Phone can be charging or fully charged. • Fast blinking green—There is a voice message. When phone is connected to the AC power source, the green light displays longer than when using only the battery. • Slow blinking green (every 2 seconds): The phone is using only battery power. The phone is registered with the wireless network and is within service coverage area. Headset port with cover Remove the protective cover and plug in a headset or ear buds.
2	Speaker button	**Speaker** Toggle the speaker mode on or off for the phone.

Item	Name or Grouping	Description
3	Softkey buttons Navigation cluster Call control buttons	Softkeys • The **More** softkey accesses a list of menus or functions. • The softkey activates the option displayed on the screen. Navigation cluster Navigation ring and **Select** button Navigation ring (outer ring): • Move up, down, left, or right in the Applications view to select these apps: • **Recents** • **Contacts** • **Apps** • **Settings** • Scroll up and down menus to highlight options and to move left and right through phone numbers and text entries. • In Line view, press left on the Navigation ring to go to the Applications view. **Select** button (center of the cluster): • Make a call from the main screen. • Select a menu item, a softkey, a call, or an action. **Answer/Send** Answer a ringing call or, after dialing a number, place the call. **Power/End Call** Turn the phone on or off, or end a connected call. When you use menus or when you are in an app, it acts as a shortcut to return to the main screen.

Item	Name or Grouping	Description
4	Keypad	Dial numbers, enter letters, and choose menu items by number. **One (1)** • Enter “1” when you dial a number. • Access voicemail. Press and hold to automatically dial the voicemail system. • Enter these special text characters: **/ . @ : ; = ? - _ & %** **Asterisk (*)** • Before you enter an international phone number, press and hold for a few seconds to add the plus (+) symbol to the phone number. • Enter these special text characters: **+ * ~ ` < >** **Zero (0)** • Enter “0” when you dial a number. • Lock the keypad. • Enter a space or these special text characters: **0 , ! ^ ' " |** **Pound (#)** • Press to silence the phone ringer. If configured, the phone will vibrate instead. • Enter these special text characters: **# $ £ ¤ ( ) { } [ ]**
5	Left Side Buttons	**Application** Use with XML applications, such as Push to Talk. **Volume** • When the phone is idle, change the ring volume or turn off the ringer. • When you have an incoming (ringing) call, press the button once to silence the ringer. • During a call, control the speaker volume for the active handset, headset, or speaker. • When the phone is docked in the desktop charger, control the volume of the charger speaker. **Mute** Toggle the mute feature on or off.

Startup Sequence

When a wireless phone powers up, the startup sequence is:

1. The red LED lights up.
2. The phone loads the firmware image that is stored in nonvolatile memory.
3. The screen turns on.
4. The phone scans for an access point.
5. The phone authenticates with the access point.
6. The phone connects with the Cisco Unified Communications Manager. If necessary, the phone obtains an updated firmware load and configuration file.

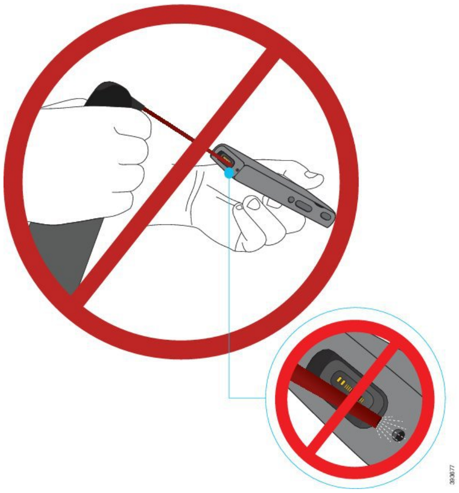
Care of Your Phone

You can clean your phone. Make sure you follow our cleaning instructions.

Clean your phone immediately if it comes in contact with anything that may cause stains, or other damage; for example, dirt or sand, ink, makeup, soap, detergent, acids, acidic foods, or lotions.

⚠

Caution Do not blow or use compressed air (for example, aerosol cans, low- or high-pressure air nozzles) to clean the openings of the phone.



Do not use a vacuum cleaner or other suction device to clean the openings of the phone.

Do not use pins or other objects to clean the openings of the phone.

Use of air, suction, or mechanical objects to clean the openings can damage the phone and voids the phone warranty.

If you happen to drop the phone into water, or it gets splashed, follow our instructions to dry off the phone. See If You Drop Your Phone in Water, on page 9.

Clean the Phone Exterior

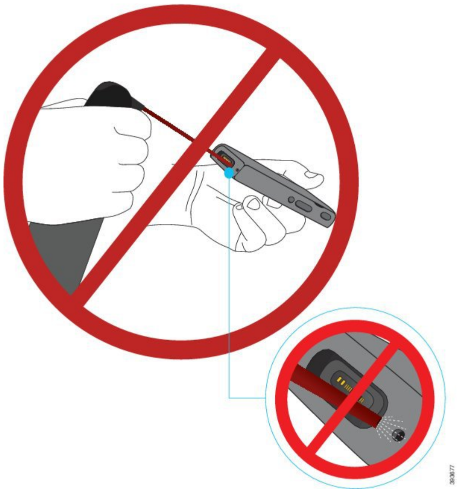
You can clean the phone exterior using a dry, lint-free cloth. For the health-care environment, we recommend that you use Caviwipes™ and Saniwipes™ to thoroughly clean the phone. Caviwipes and Saniwipes contain up to 17% isopropanol.

Any cleaning solution containing a higher amount of isopropanol, including pure isopropanol, or an alternative alcohol-based liquid could potentially damage the phone. Do not clean the phone with bleach or other caustic products.

Excessive use of Caviwipes and Saniwipes more than 3 times a day will damage the phone surface coating and will change the appearance of phone.

Clean your phone immediately if it comes in contact with anything that may cause stains, or other damage; for example, dirt or sand, ink, makeup, soap, detergent, acids, acidic foods, or lotions.

⚠ **Caution** Do not blow or use compressed air (for example, aerosol cans, low- or high-pressure air nozzles) to clean the openings of the phone.



Do not use a vacuum cleaner or other suction device to clean the openings of the phone.

Do not use pins or other objects to clean the openings of the phone.

Use of air, suction, or mechanical objects to clean the openings can damage the phone and voids the phone warranty.

Do not submerge the phone in any liquid.

Do not use a heavily-saturated cloth.

Procedure

Step 1 Remove the phone from the charger or unplug it from the charging cable.

Step 2 If the phone is in a protective case, remove the phone from the case.

Step 3 Wipe the phone and screen with a damp, soft, lint-free cloth.

Step 4 If there are foreign objects (for example, fine sand) in an opening in the phone, tap the phone against your hand to dislodge the objects.

If You Drop Your Phone in Water

If you drop your phone in water, here's what you do:

- *Gently* shake the water off the phone.
- Dry the phone with a soft, dry, lint-free cloth.
- Leave your phone in a dry area with some air flow; for example, a fan blowing *cool* air can be directed onto the phone speaker grill to help the phone dry out. Just don't put the fan close to the phone.

Here are some things you don't do:

- Don't open the battery door while the phone is wet.
- Don't use compressed air to blow off the water.
- Don't use a hair dryer to dry off the phone.
- Don't put a cotton swab, paper towel, or cloth into the headset jack or inside the battery compartment.
- Don't tap the phone on a hard surface.
- Don't charge a wet phone using the charging cable. You must wait until the phone is completely dry.
- Don't put a wet phone into the desktop charger, or multicharger. You must wait until the phone is completely dry.

⚠

Caution Do not blow or use compressed air (for example, aerosol cans, low- or high-pressure air nozzles) to clean the openings of the phone.

Do not use a vacuum cleaner or other suction device to clean the openings of the phone.

Do not use pins or other objects to clean the openings of the phone.

Use of air, suction, or mechanical objects to clean the openings can damage the phone and voids the phone warranty.

⚠

Caution To ensure that the phone does not get water into the battery compartment, make sure that the compartment is tightly closed. See Install the Cisco Wireless IP Phone 8821 Battery, on page 35.

If the sound is muffled after you dry the phone, there may still be water in the microphone or speaker compartments. Place your phone, speaker-side down, on a dry, lint-free cloth to see if water drips out. If there is still water in the phone, allow the phone to completely dry before you use it.

Best Practices for Battery Power Conservation

The Cisco Wireless IP Phone 8821 and 8821-EX has a 2060-mAh smart battery. The battery capacity is reduced to 80% after 500 full charging cycles (charging from empty to full). The battery life also depends on the phone state, the frequency and AP scanning configuration.

Table 1: Battery Life

Call State	Scan Mode	Expected Battery Time
On-Call	Continuous	Up to 9.5 hours
	Auto	Up to 9.5 hours

Call State	Scan Mode	Expected Battery Time
Idle	Continuous	Up to 45 hours
	Auto	Up to 145 hours

For more information on batteries, see the *Cisco Wireless IP Phone 882x Series Accessory Guide*.

Follow these best practices to ensure that the phone conserves battery power.

User Actions

Remind your users that the battery life is reduced when the phone is turned on. Calls, messages, application use, Bluetooth use, and actions like menu navigation use power.

Users should ensure that the phone remains in a good RF coverage area and that the phone can maintain a constant connection to the Cisco Unified Communications Manager. If the phone moves out of range and remains out of range for a significant time, battery life can be reduced.

For more information about RF coverage, see Cisco Wireless IP Phone 882x Deployment Guide, on page 22.

Phone Configuration

Configure the Scan mode field in Cisco Unified Communications Manager to suit your enterprise. The phone supports Continuous, Auto, and Single AP scanning, where Continuous is the default. The configured scan mode determines the battery life baseline.

- Continuous scan mode is designed for phone users that are constantly on the move and for whom frequent roaming events occur. This mode maximizes performance and connectivity, but at the expense of battery power.
- Auto scan mode is designed for phone users that only roam occasionally, and whoe require more idle battery life than Continuous scan mode can offer.
- Single AP scan mode is designed for phone users that do not roam and require maximum idle battery life.

Access Point Configuration

- For optimal idle battery life, we recommend that you use an access point that supports the Cisco Compatible Extensions (CCX) Proxy ARP feature. CCX Proxy ARP allows the phone to remain in suspend mode longer instead of waking up at each DTIM period. This reduces power consumption.

  The Cisco Lightweight Access Points and Cisco Autonomous Access Points support CCX Proxy ARP, but Cisco Meraki Access Points do not.

  For Cisco Lightweight Access Points, CCX Proxy ARP is enabled by default and nonconfigurable. For Cisco Autonomous Access Points, CCX Proxy ARP is disabled by default, but can be enabled with the **`dot11 arp-cache`** optional command.

  If the access point does not support CCX Proxy ARP, then the phone must wake up at each DTIM period. Frequent wakeups can reduce the idle battery life by as much as 50%.
- We recommend that you use an access point that supports the Cisco Compatible Extensions (CCX) Dynamic Transmit Power Control (DTPC) feature. When DTPC is enabled, the access point advertises

its transmit power to all clients. The phone adjusts its transmit power to the minimum level necessary to communicate with the access point. A lower transmit power reduces unnecessary noise in other areas.

- Limit the use of multicast. If the phone subscribes to a multicast stream, it wakes up at each DTIM period to receive multicast frames. Frequent wake-ups cause power consumption to increase.
- Select an access point that supports U-APSD. This power save protocol is used when on call and when idle.
  - The On Call Power Save field in the Wi-Fi Profile should remain enabled so that the phone can use U-APSD.
  - If the On Call Power Save field is disabled, then the phone uses active mode when on call, but uses U-APSD when in idle mode.

Only disable On Call Power Save for troubleshooting purposes.

New and Changed Information

New and Changed Information for Cisco Wireless IP Phone 8821-EX Support

The following updates were made to the document.

Feature	Description
Cisco Wireless IP Phone 8821-EX Support	Cisco Wireless IP Phone 8821 and 8821-EX, on page 1 Install the Cisco Wireless IP Phone 8821-EX Battery, on page 40 Replace the Cisco Wireless IP Phone 8821-EX Battery, on page 49 Supported Accessories, on page 103 Desktop Chargers, on page 104 Multichargers, on page 108

New and Changed Information for Firmware Release 11.0(5)SR1

The following updates were made to the document.

Feature	Description
Wi-Fi authentication method corrections	Network Protocols, on page 20 Set Up a Wi-Fi Profile using Cisco Unified Communications Manager, on page 62 Bulk Deployment Utility, on page 66 Authentication Failed, No AP Found, on page 141 Phone Loses Cisco Unified Communications Manager Connection While Roaming, on page 150

New and Changed Information for Firmware Release 11.0(5)

The following table describes changes to this book to support Firmware Release 11.0(5).

Feature Name	Updates
Configuration Cleanup	Several fields removed in Product Specific Configuration Fields, on page 70
New Chargers for the Cisco Wireless IP Phone 8821	Supported Accessories, on page 103 Desktop Chargers, on page 104 Multichargers, on page 108
Security Enhancements	New **Disable TLS 1.0 and TLS 1.1 for Web Access** field added to Product Specific Configuration Fields, on page 70 Cisco Discovery Protocol (CDP) added to Network Protocols, on page 20
Serviceability Enhancements	• New **Customer Support Upload URL** field added to Product Specific Configuration Fields, on page 70 • Problem Report Tool, on page 77 • Manage Core Dumps from the Admin Web Page, on page 136 • Perform Audio Diagnostics, on page 155 • Generate a Problem Report from the Admin Web Page, on page 157
User Interface Enhancements	New **Divert Alerting Call** and **Allow Vibrate URI When On Call** fields added to Product Specific Configuration Fields, on page 70 All references to IPv6 have been removed. Access Device Information, on page 113 Device Information Web Page, on page 123

Feature Name	Updates
As a result of recent changes to the hardware, the Cisco Wireless IP Phone 8821 is now certified for IP54 ingress protection, and is no longer certified for IP67 ingress protection.	Cisco Wireless IP Phone 8821 and 8821-EX, on page 1 Install the Cisco Wireless IP Phone 8821 Battery, on page 35 Replace the Cisco Wireless IP Phone 8821 Battery, on page 44 Physical and Operating Environment, on page 161

New and Changed Information for Firmware Release 11.0(4)

The following table describes changes to this book to support Firmware Release 11.0(4).

Feature Name	Updates
Configurable home screen	Buttons and Hardware, on page 3 Product Specific Configuration Fields, on page 70 As well, references to the home screen have been updated for Applications and Line view home screens.
Local contacts	Local Contacts Management from the Phone Administration Page, on page 95
Problem report tool	Problem Report Tool Create a Problem Report from the Phone, on page 156
Resized wallpapers	Custom Background Images, on page 83 and its subsections
User interface enhancements	WMM UP statistics added to Call Statistics, on page 121 and Streaming Statistics Web Page, on page 128.
General changes	Phone Statistics in the Admin Settings Menu, on page 119 Boot the Phone to the Alternate Firmware, on page 131 Reset the Phone to Factory Defaults from the Phone Keypad, on page 132 Access Phone Diagnostics Find the List of Neighbor Access Points, on page 156 Best Practices for Battery Power Conservation, on page 10

New and Changed Information for Firmware Release 11.0(3)SR4

The following table contains the information that was added or changed in this book for this firmware release.

Feature	Updates
Bulk Deployment Utility	Bulk Deployment Utility, on page 66

New and Changed Information for Firmware Release 11.0(3)

The following table contains the information that was added or changed in this book for this firmware release.

Feature	Updates
FIPS 140-2 Level 1 Support	Feature removed in 11.0(5).
Power Saving Enhancements	Best Practices for Battery Power Conservation, on page 10

Phone Firmware

The factory installs a version of the phone firmware on the phone during manufacturing. But that firmware may not be the latest firmware version.

Your Cisco Unified Communications Manager stores the firmware loads. If the version of firmware on the phone is not the latest version, the Cisco Unified Communications Manager sends the updated firmware load to the phone.

Device Packs

The Cisco Unified Communication Manager Device Pack contains device configuration capabilities for the phones. Many phone features require the latest device package to be installed on the Cisco Unified Communications Manager. If you do not install the device pack, the new phone features do not work.

A device pack introduces new phone types to Cisco Unified Communication Manager. The pack installs the firmware and the configuration files needed to enable features on your phone. New features may be turned off by default and they have attributes or settings that must be configured.

To find which device packs are available for your Cisco Unified Communications Manager version and phone, go to: http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/compat/devpack_comp_mtx.html

Phone Configuration Files

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

Configuration files also contain information about which image load the phone should be running. If this image load differs from the one currently loaded on a phone, the phone contacts the TFTP server to request the required load files.

If you configure security-related settings in Cisco Unified Communications Manager Administration, the phone configuration file will contain sensitive information. To ensure the privacy of a configuration file, you must configure it for encryption. For more information, see the documentation for your particular Cisco Unified Communications Manager release. A phone requests a configuration file whenever it resets and registers with Cisco Unified Communications Manager.

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

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

Related Documentation

Use the following sections to obtain related information.

Cisco Wireless IP Phone 882x Series Documentation

Refer to publications that are specific to your language, phone model, and call control system. Navigate from the following documentation URL:

https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/tsd-products-support-series-home.html

The Deployment Guide is located at the following URL:

https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-implementation-design-guides-list.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:

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html

Cisco Unified Communications Manager Express Documentation

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

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-express/tsd-products-support-series-home.html

Cisco Business Edition 6000 Documentation

Refer to the *Cisco Business Edition 6000 Documentation Guide* and other publications that are specific to your Cisco Business Edition 6000 release. Navigate from the following URL:

https://www.cisco.com/c/en/us/support/unified-communications/business-edition-6000/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/c/en/us/td/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 IP Phone User Support

If you are a system administrator, you are likely the primary source of information for Cisco IP Phone users in your network or company. It is important to provide current and thorough information to end users.

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

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

Consider including the following types of information on this site:

- User guides for all Cisco IP Phone models that you support
- Information on how to access the Cisco Unified Communications Self Care Portal
- List of features supported
- User guide or quick reference for your voicemail system

CHAPTER 2

VoIP Networks

Network Requirements

For the phone to successfully operate as an endpoint in your network, your network must meet the following requirements:

- VoIP Network
  - VoIP is configured on your Cisco routers and gateways.
  - Cisco Unified Communications Manager is installed in your network and is configured to handle call processing.
- IP network that supports DHCP or manual assignment of IP address, gateway, and subnet mask
- Wireless LAN
  - Access Points (APs) are configured to support voice over WLAN.
  - Controllers and switches are configured to support voice.
  - Security is implemented for authenticating wireless voice devices and users.

Note The phone displays the date and time from Cisco Unified Communications Manager. If the user turns off **Automatic date and time** in the Settings application, the time may become out of sync with the server time.

Network Protocols

The Cisco Wireless IP Phone 8821 and 8821-EX supports several industry-standard and Cisco network protocols required for voice communication. The following table provides an overview of the network protocols that the phones support.

Table 2: Supported Network Protocols

Network protocol	Purpose	Usage notes
Bluetooth	Bluetooth is a wireless personal area network (WPAN) protocol that specifies how devices communicate over short distances.	The phones support Bluetooth 4.0.
Bootstrap Protocol (BootP)	BootP enables a network device, such as the Cisco IP Phone, to discover certain startup information, such as the IP address.	None
Cisco Audio Session Tunnel (CAST)	The CAST protocol allows Cisco IP Phones and associated applications to discover and communicate with the remote IP Phones without requiring changes to the traditional signaling components, such as Cisco Unified Communications Manager (CM) and gateways.	The phones use CAST as an interface between CUVA and Cisco Unified Communications Manager using the Cisco IP Phone as a SIP proxy.
Cisco Discovery Protocol (CDP)	CDP is a device-discovery protocol that runs on all Cisco-manufactured equipment. Using CDP, a device can advertise its existence to other devices and receive information about other devices in the network.	The phones use CDP to communicate information such as auxiliary VLAN ID, per port power management details, and Quality of Service (QoS) configuration information with the Cisco Catalyst switch.
Cisco Peer-to-Peer Distribution Protocol (CPPDP)	CPPDP is a Cisco proprietary protocol used to form a peer-to-peer hierarchy of devices. This hierarchy is used to distribute firmware files from peer devices to their neighboring devices.	CPPDP is used by the Peer Firmware Sharing feature.
Dynamic Host Configuration Protocol (DHCP)	DHCP dynamically allocates and assigns an IP address to network devices. DHCP enables you to connect an IP phone into the network and the phone to become operational without the need to manually assign an IP address or to configure additional network parameters.	DHCP is enabled by default. If disabled, you must manually configure the IP address, subnet mask, gateway, and a TFTP server on each phone locally. We recommend that you use DHCP custom option 150. With this method, you configure the TFTP server IP address as the option value. For more information, see the documentation for your particular Cisco Unified Communications Manager release. **Note** If you cannot use option 150, you may try using DHCP option 66.
Hypertext Transfer Protocol (HTTP)	HTTP is the standard way of transferring information and moving documents across the Internet and the web.	The phones use HTTP for XML services and for troubleshooting purposes.

Network protocol	Purpose	Usage notes
Hypertext Transfer Protocol Secure (HTTPS)	Hypertext Transfer Protocol Secure (HTTPS) is a combination of the Hypertext Transfer Protocol with the SSL/TLS protocol to provide encryption and secure identification of servers.	Web applications with both HTTP and HTTPS support have two URLs configured. Phones that support HTTPS choose the HTTPS URL.
IEEE 802.1X	The IEEE 802.1X standard defines a client-server-based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. Until the client is authenticated, 802.1X access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.	The phones implement the IEEE 802.1X standard by providing support for the following authentication methods: • EAP-FAST • EAP-TLS • PEAP-GTC • PEAP-MSCHAPV2
IEEE 802.11n/802.11ac	The IEEE 802.11 standard specifies how devices communication over a wireless local area network (WLAN).	802.11n operates in the 2.4 GHz and 5 GHz band. 802.11ac operates in the 5 GHz band.
Internet Protocol (IP)	IP is a messaging protocol that addresses and sends packets across the network.	To communicate using IP, network devices must have an assigned IP address, subnet, and gateway. IP addresses, subnets, and gateway identifications are automatically assigned if you are using the phone with Dynamic Host Configuration Protocol (DHCP). If you are not using DHCP, you must manually assign these properties to each phone locally. The phones do not support IPv6.
Real-Time Transport Protocol (RTP)	RTP is a standard protocol for transporting real-time data, such as interactive voice, over data networks.	The phones use the RTP protocol to send and receive real-time voice traffic from other phones and gateways.
Real-Time Control Protocol (RTCP)	RTCP works in conjunction with RTP to provide QoS data (such as jitter, latency, and round-trip delay) on RTP streams.	RTCP is enabled by default.
Session Description Protocol (SDP)	SDP is the portion of the SIP protocol that determines which parameters are available during a connection between two endpoints. Conferences are established by using only the SDP capabilities that all endpoints in the conference support.	SDP capabilities, such as codec types, DTMF detection, and comfort noise, are normally configured on a global basis by Cisco Unified Communications Manager or Media Gateway in operation. Some SIP endpoints may allow configuration of these parameters on the endpoint itself.

Network protocol	Purpose	Usage notes
Session Initiation Protocol (SIP)	SIP is the Internet Engineering Task Force (IETF) standard for multimedia conferencing over IP. SIP is an ASCII-based application-layer control protocol (defined in RFC 3261) that can be used to establish, maintain, and terminate calls between two or more endpoints.	Like other VoIP protocols, SIP addresses the functions of signaling and session management within a packet telephony network. Signaling allows transportation of call information across network boundaries. Session management provides the ability to control the attributes of an end-to-end call.
Transmission Control Protocol (TCP)	TCP is a connection-oriented transport protocol.	The phones use TCP to connect to Cisco Unified Communications Manager and to access XML services.
Transport Layer Security (TLS)	TLS is a standard protocol for securing and authenticating communications.	Upon security implementation, the phones use the TLS protocol when securely registering with Cisco Unified Communications Manager.
Trivial File Transfer Protocol (TFTP)	TFTP allows you to transfer files over the network. On the Cisco IP Phone, TFTP enables you to obtain a configuration file specific to the phone type.	TFTP requires a TFTP server in your network that the DHCP server can automatically identify. If you want a phone to use a TFTP server other than the one that the DHCP server specifies, you must manually assign the IP address of the TFTP server by using the Network Configuration menu on the phone. For more information, see the documentation for your particular Cisco Unified Communications Manager release.
User Datagram Protocol (UDP)	UDP is a connectionless messaging protocol for delivery of data packets.	UDP is used by the phones for signaling.

Related Topics

Manually Set Up the Phone Network from the Settings Menu , on page 87
Cisco Unified Communications Manager Interaction, on page 32
802.11 Standards for WLAN Communications, on page 27
Startup Sequence, on page 7

Cisco Wireless IP Phone 882x Deployment Guide

The *Cisco Wireless IP Phone 882x Deployment Guide* contains useful information about the wireless phone in the Wi-Fi environment. You can find the deployment guide at this location:

https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-implementation-design-guides-list.html

Wireless LAN

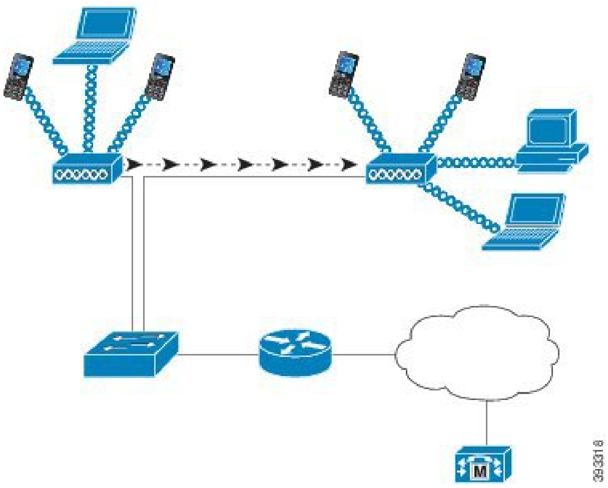
Note For detailed Cisco Wireless IP Phone 8821 and 8821-EX deployment and configuration instructions, see the *Cisco Wireless IP Phone 8821 Series Deployment Guide*.

Devices with wireless capability can provide voice communication within the corporate WLAN. The device depends on and interacts with wireless access points (AP) and key Cisco IP Telephony components, including Cisco Unified Communications Manager Administration, to provide wireless voice communication.

The wireless phones exhibit Wi-Fi capabilities that can use 802.11a, 802.11b, 802.11g, and 802.11n Wi-Fi.

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

Figure 3: Typical WLAN Topology



When a phone powers on, it searches for and associates with an AP if the device wireless access is set to On. If remembered networks are not within range, you can select a broadcasted network or manually add a network.

The AP uses the connection to the wired network to transmit data and voice packets to and from the switches and routers. Voice signaling is transmitted to the call control 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. In some WLANs, each AP has a wired connection to an Ethernet switch, such as a Cisco Catalyst 3750, that is configured on a LAN. The switch provides access to gateways and the call control server to support wireless IP telephony.

Some networks contain wired components that support wireless components. The wired components can comprise switches, routers, and bridges with special modules to enable wireless capability.

For more information about Cisco Unified Wireless Networks, see https://www.cisco.com/c/en/us/products/wireless/index.html.

Wi-Fi Network Components

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

AP Channel and Domain Relationships

Access points (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.

For more information about AP channel and domain relationships, see the “Designing the Wireless LAN for Voice” section in the *Cisco Wireless IP Phone 8821 Series Deployment Guide*.

AP Interactions

Wireless 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 can make the call inaudible. Packet errors can also cause blocky or frozen video.

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

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

After deploying and using wireless voice, you should continue to perform 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 is still adequate for optimal voice communications.

Note Packet loss occurs during roaming; however, the security mode and the presence of fast roaming determines how many packets are lost during transmission. Cisco recommends implementation of Cisco Centralized Key Management (CCKM) to enable fast roaming.

For more information about Voice QoS in a wireless network, see the *Cisco Wireless IP Phone 8821 Series Deployment Guide*.

Access Point Association

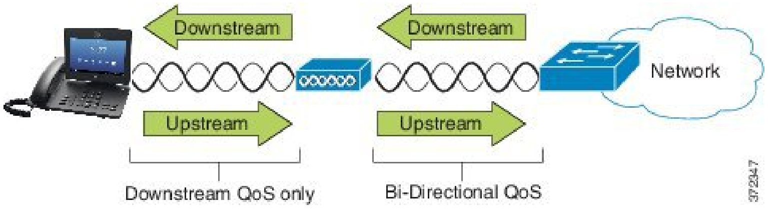
At startup, the phone scans for APs with SSIDs and encryption types that it recognizes. The phone builds and maintains a list of eligible APs and selects the best AP, based on the current configuration.

QoS in a Wireless Network

Voice and video 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 can seriously impact a voice or video call. To ensure that voice and video traffic receives timely and reliable treatment with low delay and low jitter, you must use Quality of Service (QoS).

By separating the devices into a voice VLAN and marking voice packets with higher QoS, you can ensure that voice traffic gets priority treatment over data traffic, which results 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 relative to the AP as shown in the following figure.



The Enhanced Distributed Coordination Function (EDCF) type of QoS has up to eight queues for downstream (toward the 802.11b/g clients) QoS. You can allocate the queues based on these options:

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

Although up to eight queues on the AP can be set up, you should use only three queues for voice, video, and signaling traffic to ensure the best possible QoS. Place voice in the Voice queue (UP6), video in the Video queue (UP5), signaling (SIP) traffic in the Video queue (UP4), and place data traffic in a best-effort queue (UP0). 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.

The queues are:

- Best Effort (BE) - 0, 3
- Background (BK) - 1, 2
- Video (VI) - 4, 5
- Voice (VO) - 6, 7

Note The device marks the SIP signaling packets with a DSCP value of 24 (CS3) and RTP packets with DSCP value of 46 (EF).

Note Call Control (SIP) is sent as UP4 (VI). Video is sent as UP5 (VI) when Admission Control Mandatory (ACM) is disabled for video (Traffic Specification [TSpec] disabled). Voice is sent as UP6 (VO) when ACM is disabled for voice (TSpec disabled).

The following table provides a QoS profile on the AP that gives priority to voice, video, and call control (SIP) traffic.

Table 3: QoS Profile and Interface Settings

Traffic Type	DSCP	802.1p	WMM UP	Port Range
Voice	EF (46)	5	6	UDP 16384-32767
Interactive Video	AF41 (34)	4	5	UDP 16384-32767
Call Control	CS3 (24)	3	4	TCP 5060-5061

To improve reliability of voice transmissions in a nondeterministic environment, the device 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. 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 issues with call quality, an initial Call Admission Control (CAC) scheme is required. With SIP CAC enabled on the WLAN, QoS is maintained in a network overload scenario by limiting the number of active voice calls so as not to exceed the configured limits on the AP. During times of network congestion, the system maintains a small bandwidth reserve so wireless device clients can roam into a neighboring AP, even when the AP is at “full capacity.” After the voice bandwidth limit is reached, the next call is load-balanced to a neighboring AP so as not to affect the quality of the existing calls on the channel.

The phones use TCP for SIP communications, and call control system registrations can potentially be lost if an AP is at full capacity. Frames to or from a client that has not been "authorized" through the CAC can be dropped, leading to call control system deregistration. Therefore, we recommend that you disable SIP CAC.

Set up Flexible DSCP

Procedure

Step 1 In Cisco Unified Communications Manager Administration, go to **System** > **Service Parameters**.

Step 2 In Clusterwide Parameters (System - Location and Region), set Use Video BandwidthPool for Immersive Video Calls to **False**.

Step 3 In Clusterwide Parameters (Call Admission Control), set Video Call QoS Marking Policy to **Promote to Immersive**.

Step 4 Save your changes.

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 wireless phones support the following standards:

- 802.11a: Uses the 5 GHz band that provides more channels and improved data rates by using OFDM technology. Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) support this standard.
- 802.11b: Specifies the radio frequency (RF) of 2.4 Ghz for both transmission and receipt of data at lower data rates (1, 2, 5.5, 11 Mbps).
- 802.11d: Enables access points to advertise their currently supported radio channels and transmit power levels. The 802.11d-enabled client then uses that information to determine the channels and powers to use. The phone requires World mode (802.11d) to determine which channels are legally allowed for any given country. For supported channels, see the table that follows. Ensure that 802.11d is properly configured on the Cisco IOS Access Points or Cisco Unified Wireless LAN Controller.
- 802.11e: Defines a set of Quality of Service (QoS) enhancements for wireless LAN applications.
- 802.11g: Uses the same unlicensed 2.4 Ghz band as 802.11b, but extends the data rates to provide greater performance by using Orthogonal Frequency Division Multiplexing (OFDM) technology. OFDM is a physical-layer encoding technology for transmission of signals through use of RF.
- 802.11h: Supports 5 GHz spectrum and transmit power management. Provides DFS and TPC to the 802.11a Media Access Control (MAC).
- 802.11i: Specifies security mechanisms for wireless networks.
- 802.11n: Uses the radio frequency of 2.4 GHz or 5 GHz for both transmission and receipt of data with speeds up to 150 Mbps, and enhances data transfer through the use of multiple input, multiple output (MIMO) technology, channel bonding, and payload optimization.

Note The wireless phones have a single antenna and use the Single Input Single Output (SISO) system, which supports MCS 0 to MCS 7 data rates only (72 Mbps with 20 MHz channels and 150 Mbps 40 MHz channels). Optionally, you can enable MCS 8 to MCS 15 if 802.11n clients are using MIMO technology that can take advantage of those higher data rates.

- 802.11r: Specifies requirements for fast secure roaming.
- 802.11ac: Uses the radio frequency of 5 GHz for both transmission and receipt of data with speeds up to 433 Mbps.

Table 4: Supported Channels

Band Range	Available Channels	Channel Set	Channel Width
2.412 - 2.472 GHz	13	1 - 13	20 MHz

Band Range	Available Channels	Channel Set	Channel Width
5.180 - 5.240 GHz	4	36, 40, 44, 48	20, 40, 80 MHz
5.260 - 5.320 GHz	4	52, 56, 60, 64	20, 40, 80 MHz
5. 500 - 5.700 GHz	11	100 - 140	20, 40, 80 MHz
5.745 - 5.825 GHz	5	149, 153, 157, 161, 165	20, 40, 80 MHz

Note Channels 120, 124, 128 are not supported in the Americas, Europe, or Japan, but may be in other regions around the world.

For information about supported data rates, Tx power and Rx sensitivity for WLANs, see the *Cisco Wireless IP Phone 8821 Series Deployment Guide*.

World Mode (802.11d)

The wireless phones use 802.11d to determine the channels and transmit power levels to use. The phone inherits its client configuration from the associated AP. Enable World mode (802.11d) on the AP to use the phone in World mode.

Note Enablement of World mode (802.11d) may not be necessary if the frequency is 2.4 GHz and the current access point is transmitting on a channel from 1 to 11.

Because all countries support these frequencies, you can attempt to scan these channels regardless of World mode (802.11d) support.

For more information on enabling World mode and 2.4 GHz support, see the *Cisco Wireless IP Phone 8821 Series Deployment Guide*.

Enable World mode (802.11d) for the corresponding country where the access point is located. World mode is enabled automatically for the Cisco Unified Wireless LAN Controller.

Radio Frequency Ranges

WLAN communications use the following radio frequency (RF) ranges:

- 2.4 GHz—Many devices that use 2.4 GHz can potentially interfere with the 802.11b/g connection. Interference can produce a Denial of Service (DoS) scenario, which may prevent successful 802.11 transmissions.
- 5 GHz—This range divides into several sections called Unlicensed National Information Infrastructure (UNII) bands, each of which has four channels. The channels are spaced at 20 MHz to provide nonoverlapping channels and more channels than 2.4 GHz provides.

Security for Communications in WLANs

Because all WLAN devices that are within range can receive all other WLAN traffic, security of voice communications is critical in WLANs. To ensure that intruders do not manipulate or intercept voice traffic, the Cisco SAFE Security Architecture supports wireless phones and Cisco Aironet APs. For more information about security in networks, see https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/index.html.

Authentication Methods

The Cisco Wireless IP Telephony solution provides wireless network security that prevents unauthorized sign-ins and compromised communications through use of the following authentication methods that wireless phones support:

- WLAN Authentication
  - WPA (802.1x authentication + TKIP or AES encryption)
  - WPA2 (802.1x authentication + AES or TKIP encryption)
  - WPA-PSK (Pre-Shared key + TKIP encryption)
  - WPA2-PSK (Pre-Shared key + AES encryption)
  - EAP-FAST (Extensible Authentication Protocol – Flexible Authentication via Secure Tunneling)
  - EAP-TLS (Extensible Authentication Protocol – Transport Layer Security)
  - PEAP (Protected Extensible Authentication Protocol) MS-CHAPv2 and GTC
  - CCKM (Cisco Centralized Key Management)
  - Open (None)
- WLAN Encryption
  - AES (Advanced Encryption Scheme)
  - TKIP / MIC (Temporal Key Integrity Protocol / Message Integrity Check)
  - WEP (Wired Equivalent Protocol) 40/64 and 104/128 bit

Note Dynamic WEP with 802.1x authentication and Shared Key authentication are not supported.

For more information about authentication methods, see the “Wireless Security” section in the *Cisco Wireless IP Phone 8821 Series Deployment Guide*.

Authenticated Key Management

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

- WPA/WPA2: Uses RADIUS server information to generate unique keys for authentication. Because these keys are generated at the centralized RADIUS server, WPA/WPA2 provides more security than WPA pre-shared keys that are stored on the AP and device.
- Cisco Centralized Key Management (CCKM): Uses RADIUS server and a wireless domain server (WDS) information 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/WPA2 and CCKM, encryption keys are not entered on the device, but are automatically derived between the AP and device. But the EAP username and password that are used for authentication must be entered on each device.

Encryption Methods

To ensure that voice traffic is secure, the wireless phones support WEP, TKIP, and Advanced Encryption Standards (AES) for encryption. When these mechanisms are used for encryption, voice Real-Time Transport Protocol (RTP) packets are encrypted between the AP and the device.

WEP

When WEP is used in the wireless network, authentication happens at the AP through 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 phones support WEP keys that use 40-bit encryption or a 128-bit encryption and remain static on the device and AP.

TKIP

WPA and CCKM use TKIP encryption, which 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 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.

For more information about encryption methods, see the “Wireless Security” section in the *Cisco Wireless IP Phone 8821 Series Deployment Guide*.

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 associates with a VLAN and the particular authentication and encryption scheme. In order for wireless phones to authenticate successfully, you must configure the same SSIDs with their authentication and encryption schemes on the APs and on the phone.

Note

- When you use 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 that are on the AP.
- The wireless phones do not support auto EAP negotiation; to use EAP-FAST mode, you must specify it.

The following table provides a list of authentication and encryption schemes that are configured on the Cisco Aironet APs that the phones support. The table shows the network configuration option for the device that corresponds to the AP configuration.

Table 5: Authentication and Encryption Schemes

Cisco WLAN Configuration			**Phone Configuration**
Authentication	**Key management**	**Common encryption**	**Authentication**
Open	None	None	None
Static WEP	None	WEP	WEP
EAP-FAST	WPA or WPA2 with optional CCKM	TKIP or AES	802.1x EAP > EAP-FAST
PEAP-MSCHAPv2	WPA or WPA2 with optional CCKM	TKIP or AES	802.1x EAP > PEAP > MSCHAPV2
PEAP-GTC	WPA or WPA2 with optional CCKM	TKIP or AES	802.1x EAP > PEAP > GTC
EAP-TLS	WPA or WPA2 with optional CCKM	TKIP or AES	802.1x EAP > TLS
WPA/WPA2-PSK	WPA-PSK or WPA2-PSK	TKIP or AES	WPA/WPA2 PSK

For more information, see the *Cisco Wireless IP Phone 8821 Series Deployment Guide*.

Certificates

The phones support the following certificates.

- X.509 digital certificate for EAP-TLS or to enable PEAP + Server Validation for WLAN authentication
- Simple Certificate Enrollment Protocol (SCEP) for certificate enrollment and auto-renewal
- 1024, 2048, 4096 bit keys
- SHA-1 and SHA-256 signature types
- DER and Base-64 (PEM) encoding types
- User Installed Certificate in PKCS #12 format (.p12 or .pfx extension), which also contains the private key
- Server (Root CA) Certificate with .crt or .cer extension

You install certificates on the phones in one of these ways:

- Use the Administration web page. For more information, see Cisco IP Phone Administration Page, on page 91.
- Use an SCEP server to manage and install the certificates. For more information, see SCEP Setup, on page 100

If your users set up their phones themselves and their phones need certificates, you need to give them the type of certificate when you give them the other configuration settings. If you don't use SCEP for certificate installation, then you need to install the certificates yourself.

WLANs and Roaming

The wireless phones support Cisco Centralized Key Management (CCKM), a centralized key management protocol that provides a cache of session credentials on the wireless domain server (WDS).

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

The phones also support 802.11r. For more information, see the *Cisco Wireless IP Phone 8821 Series Deployment Guide*.

Cisco Unified Communications Manager Interaction

Cisco Unified Communications Manager is an open, industry-standard call processing system. Cisco Unified Communications Manager software sets up and tears down calls between phones, integrating traditional PBX functionality with the corporate IP network. Cisco Unified Communications Manager manages the components of the IP telephony system, such as the phones, the access gateways, and the resources necessary for features such as call conferencing and route planning. Cisco Unified Communications Manager also provides:

- Firmware for phones
- Certificate Trust List (CTL) and Identity Trust List (ITL) files using the TFTP and HTTP services
- Phone registration
- Call preservation, so that a media session continues if signaling is lost between the primary Communications Manager and a phone

For information about configuring Cisco Unified Communications Manager to work with the IP phones described in this chapter, see the documentation for your particular Cisco Unified Communications Manager release.

Note If the Cisco IP Phone model that you want to configure does not appear in the Phone Type drop-down list in Cisco Unified Communications Manager Administration, install the latest support patch for your version of Cisco Unified Communications Manager from Cisco.com.

Voice Messaging System Interaction

Cisco Unified Communications Manager lets you integrate with different voice messaging systems, including the Cisco Unity Connection voice messaging system. Because you can integrate with various systems, you must provide users with information about how to use your specific system.

To enable the ability for a user to transfer to voicemail, set up a *xxxxx dialing pattern and configure it as Call Forward All to Voicemail. For more information, see the Cisco Unified Communications Manager documentation.

Provide the following information to each user:

- How to access the voice messaging system account.
- Initial password for accessing the voice messaging system.

  Configure a default voice messaging system password for all users.
- How the phone indicates that voice messages are waiting.

  Use Cisco Unified Communications Manager to set up a message waiting indicator (MWI) method.

CHAPTER 3

Phone Setup

Phone Hardware Installation

Before you can use your phone, you must install and charge the battery. The battery may already be installed in your phone, or you may have to install it yourself.

You must read the safety information in Product Safety and Security, on page 165 before you use, install, or charge the phone.

The battery may already be charged using one of the supported charging methods. If the battery isn't charged, you must charge the battery before you can set up the phone.

⚠

Caution The Cisco Wireless IP Phone 8821 and the Cisco Wireless IP Phone 8821-EX have different ways to lock the battery compartment. Use the correct procedures for your phone.

- Cisco Wireless IP Phone 8821
  - Install the Cisco Wireless IP Phone 8821 Battery, on page 35
  - Replace the Cisco Wireless IP Phone 8821 Battery, on page 44
- Cisco Wireless IP Phone 8821-EX
  - Install the Cisco Wireless IP Phone 8821-EX Battery, on page 40
  - Replace the Cisco Wireless IP Phone 8821-EX Battery, on page 49

Install the Cisco Wireless IP Phone 8821 Battery

Use this task for the Cisco Wireless IP Phone 8821 only. For the Cisco Wireless IP Phone 8821-EX, see Install the Cisco Wireless IP Phone 8821-EX Battery, on page 40.

IP54 compliance mean that the phone is sealed from dust and water. When the phone leaves the factory, it is completely sealed.

If you need to open the battery compartment, don't open it in a dusty or wet environment.

You should make sure that the battery cover is closed to ensure that dust and water cannot enter the battery compartment.

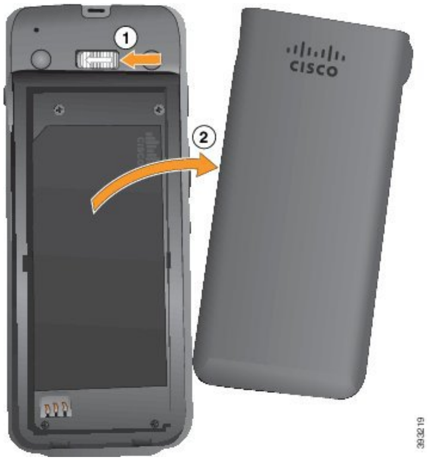
Note Dirt, oil, or other products can damage the gasket on the battery compartment cover, resulting in a poor seal. Every time you change the battery, inspect the gasket for damage. If the gasket is damaged, you can order a replacement cover.

Caution Phone life and functions could be compromised if:

- The battery is installed incorrectly.
- The battery cover is not closed properly.
- The rubber gasket on battery cover is poorly maintained.
- The rubber gasket on battery cover is damaged.
- The phone is dropped on a hard surface on a regular basis.

Procedure

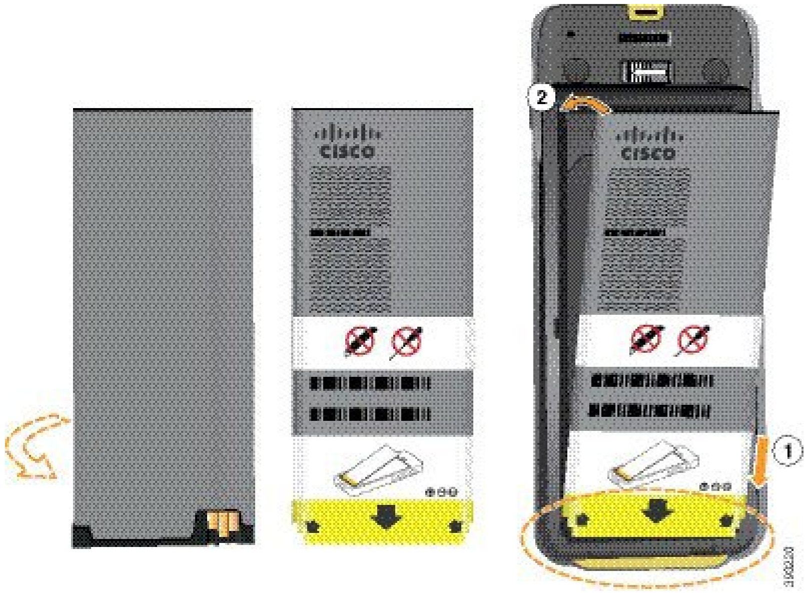
Step 1 Remove the cover from the battery compartment.



a) Push and hold the locking catch to the left to release the cover.
b) Use the tabs on the sides of the cover to lift the top of the cover and lift the cover up to unlock the bottom tabs .

Step 2 Install the battery.

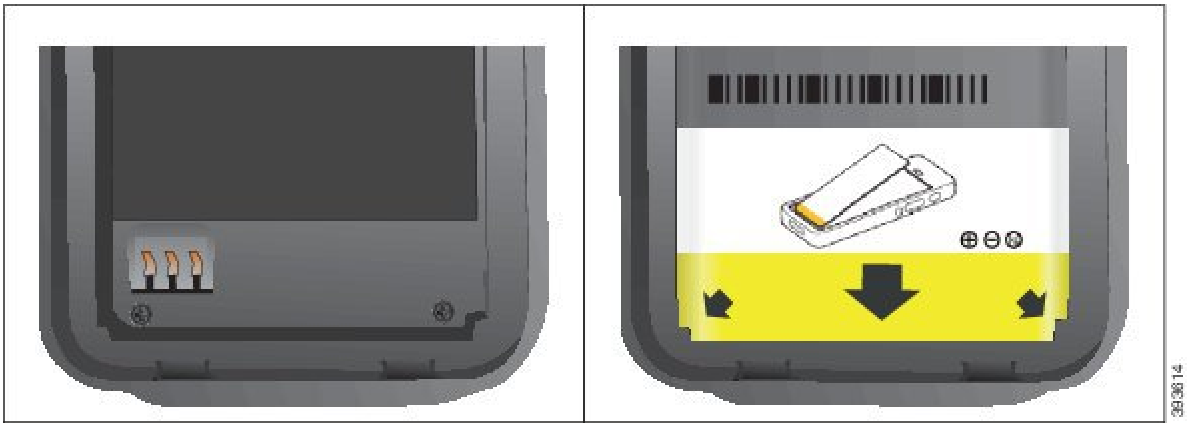
Caution If you install the battery incorrectly in the battery compartment, the battery and the battery compartment will be damaged.



The battery has metal contacts that must connect to the contacts in the battery compartment. The battery also has an arrow at the bottom and the Cisco logo at the top.

When the battery is correctly inserted, the logo and arrow are visible. The arrow points towards the connector on the base of the phone and the logo is close to the locking catch.

The battery compartment has small tabs in the bottom corners. The battery must slide under these tabs. The following graphic shows the battery compartment without and with the battery correctly installed.



a) Hold the battery so that the lower edge is close to the bottom of the compartment. Make sure that the metal contacts on the phone and battery face each other. On the battery, the Cisco logo must be near the locking catch and the arrow must point to the base of the phone.

Caution Do not force the battery into the compartment or you will damage the compartment and the battery.

b) Slide the bottom of the battery under the tabs in the bottom of the battery compartment.

c) Press the battery into the battery compartment until it is flat in the compartment.

The following graphic shows a properly-installed battery.

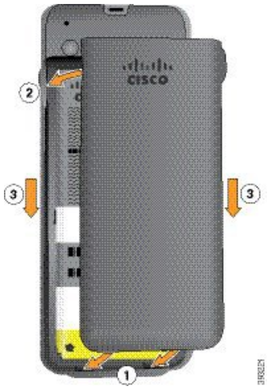
cisco
393612

d) If the battery has a light plastic pull tab, the tab should be flat in the compartment.

Step 3 Inspect the gasket on the inside of the battery compartment cover and, if necessary, clean it with a cloth dampened with water.

Caution Do not use oil- or alcohol-based cleaners on the gasket. These cleaners will damage the gasket and void the phone warranty.

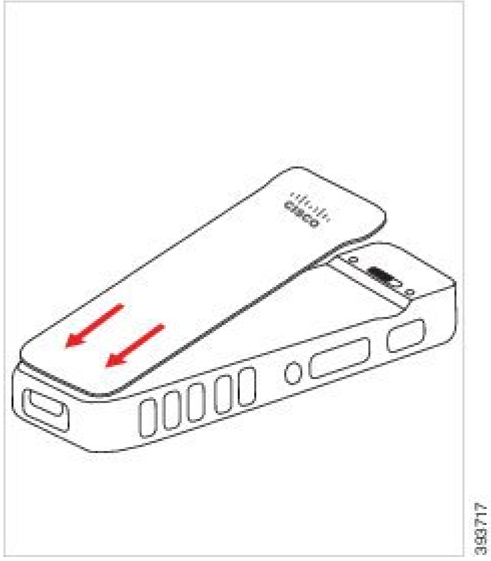
Step 4 Replace the cover to the battery compartment.



Caution When you close the battery cover, make sure that it is completely closed. Otherwise dust and water can enter the battery compartment.

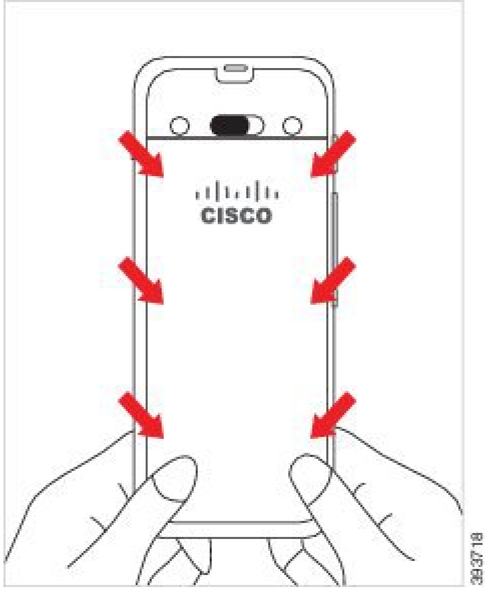
a) Align the tabs at the bottom of the cover into the notches on the phone.

The tabs slide into the phone.



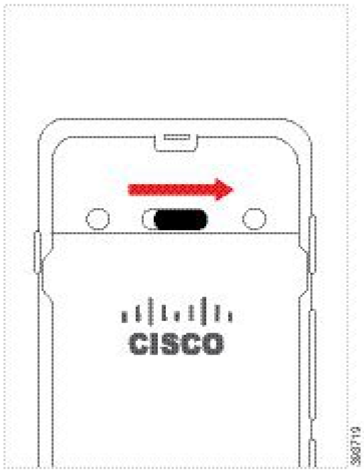
b) Press the cover firmly against the phone until it clicks in place. Press at the top, middle, and bottom of the cover on each side.

Press the cover firmly.



Caution Do not force the cover. If it doesn't click into place easily, remove the cover and check that the battery is inserted correctly.

c) Check that the cover is flush with the phone, then slide the lock to the right to lock the cover in place.



Install the Cisco Wireless IP Phone 8821-EX Battery

Use this task for the Cisco Wireless IP Phone 8821-EX only. For the Cisco Wireless IP Phone 8821, see Install the Cisco Wireless IP Phone 8821 Battery, on page 35.

IP67 compliance mean that the phone is sealed from dust and water. When the phone leaves the factory, it is completely sealed.

Caution If you need to open the battery compartment, don't open it in a dusty or wet environment or in a hazardous location.

Don't open the compartment if the temperature is 0°C or less.

You should make sure that the battery cover is closed to ensure that dust and water cannot enter the battery compartment.

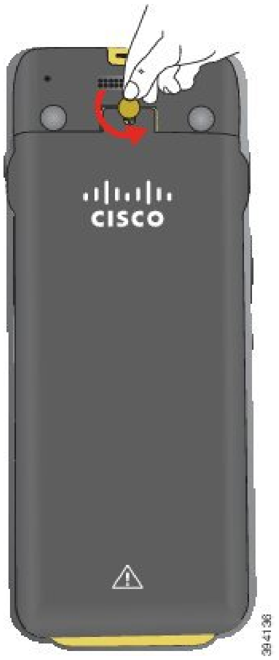
Note Dirt, oil, or other products can damage the gasket on the battery compartment cover, resulting in a poor seal. Every time you change the battery, inspect the gasket for damage. If the gasket is damaged, you can order a replacement cover.

Caution Phone life and functions could be compromised if:

- The battery is installed incorrectly.
- The battery cover is not closed properly.
- The rubber gasket on battery cover is poorly maintained.
- The rubber gasket on battery cover is damaged.
- The phone is dropped on a hard surface on a regular basis.

Procedure

Step 1 Use a coin to unscrew the battery cover and remove the cover from the battery compartment.



Caution Don't use a sharp object to unscrew the battery compartment door or to pry the battery door off the phone.

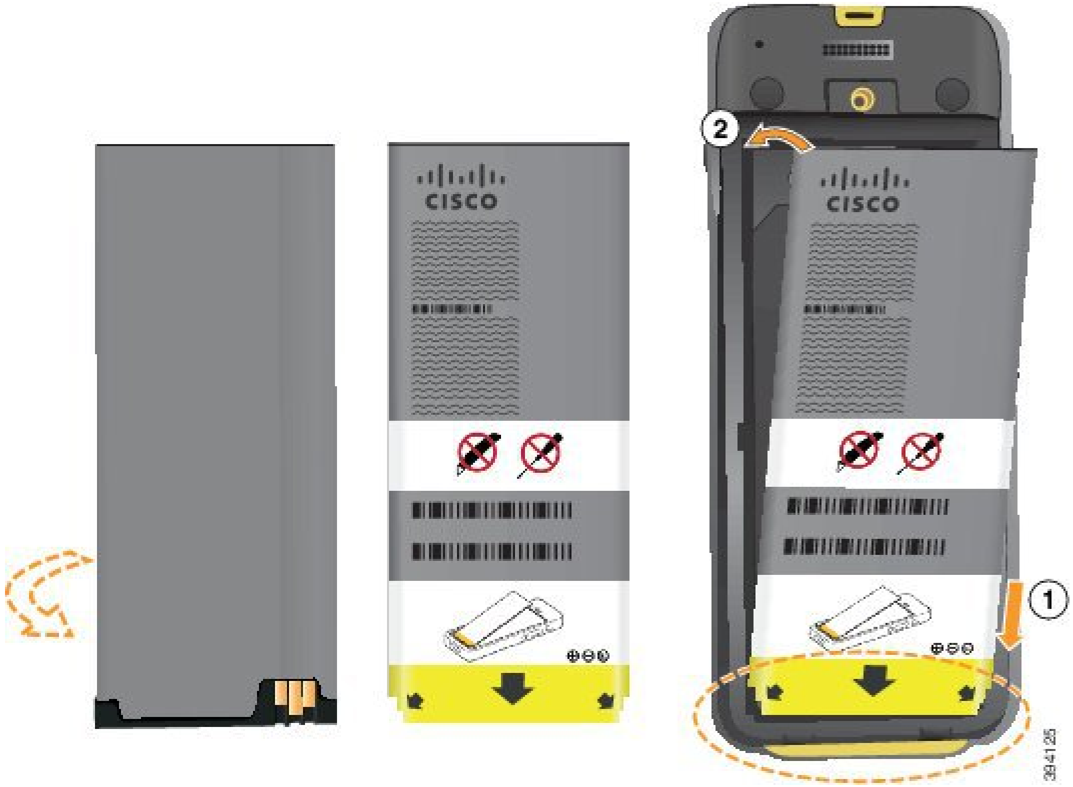
a) Use a coin to turn the screw and unlock the battery compartment.

The screw remains in the cover.

b) Lift and remove the cover of the battery compartment with your fingers, *one corner at a time*.

Step 2 Install the battery.

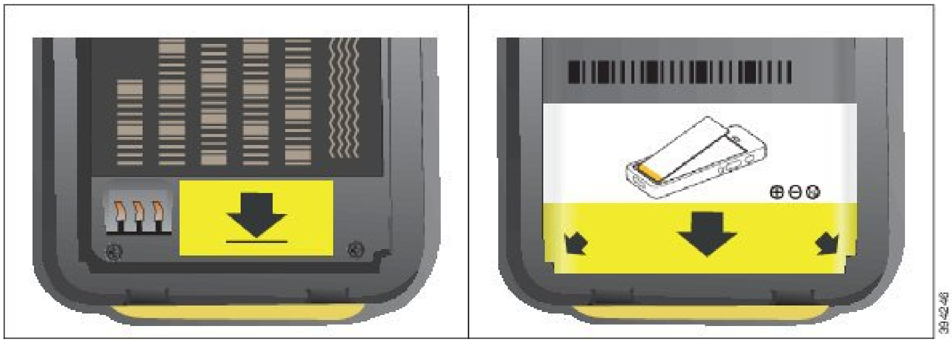
Caution If you install the battery incorrectly in the battery compartment, the battery and the battery compartment will be damaged.



The battery has metal contacts that must connect to the contacts in the battery compartment. The battery also has an arrow at the bottom and the Cisco logo at the top.

When the battery is correctly inserted, the logo and arrow are visible. The arrow points towards the connector on the base of the phone and the logo is close to the locking catch.

The battery compartment has small tabs in the bottom corners. The battery must slide under these tabs. The following graphic shows the battery compartment without and with the battery correctly installed.



a) Hold the battery so that the lower edge is close to the bottom of the compartment. Make sure that the metal contacts on the phone and battery face each other. On the battery, the Cisco logo must be near the locking catch and the arrow must point to the base of the phone.

Caution Do not force the battery into the compartment or you will damage the compartment and the battery.

b) Slide the bottom of the battery under the tabs in the bottom of the battery compartment.

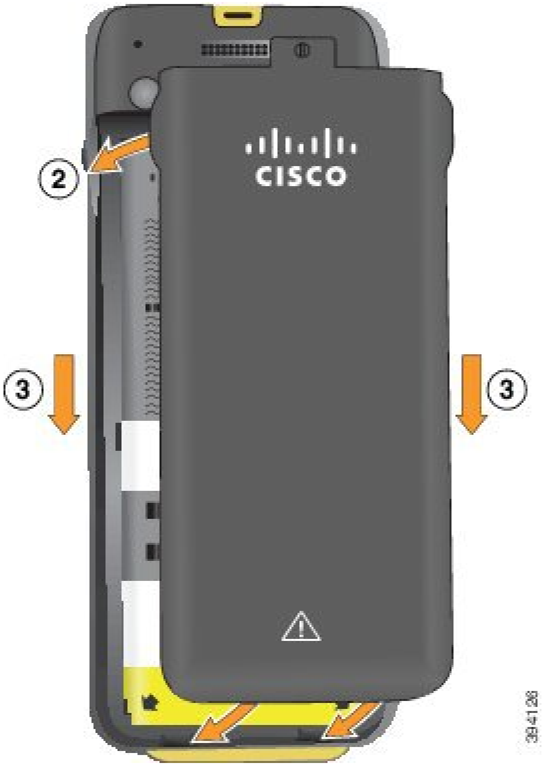
c) Press the battery into the battery compartment until it locks in place. Make sure that is flat in the compartment.

d) If the battery has a light plastic pull tab, the tab should be flat in the compartment.

Step 3 Inspect the gasket on the inside of the battery compartment cover and, if necessary, clean it with a cloth dampened with water.

Caution Do not use oil- or alcohol-based cleaners on the gasket. These cleaners will damage the gasket and void the phone warranty.

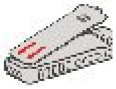
Step 4 Replace the cover to the battery compartment.



Caution When you close the battery cover, make sure that it is completely closed. Otherwise dust and water can enter the battery compartment.

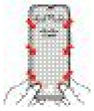
a) Align the tabs at the bottom of the cover into the notches on the phone.

The tabs slide into the phone.



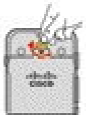
b) Press the cover firmly against the phone until it clicks in place.

Press at the top, middle, and bottom of the cover on each side.



Caution Do not force the cover down. If it doesn't click into place easily, remove the cover and check that the battery is inserted correctly.

c) Check that the cover is flush with the phone, then use a coin to screw the cover in place. The screw should be snug. Don't make it too tight.



Replace the Cisco Wireless IP Phone 8821 Battery

Use this task for the Cisco Wireless IP Phone 8821 only. For the Cisco Wireless IP Phone 8821-EX, see Replace the Cisco Wireless IP Phone 8821-EX Battery, on page 49.

If you have a spare battery, you can replace a depleted battery with a charged battery.

IP54 compliance mean that the phone is sealed from dust and water. When the phone leaves the factory, it is completely sealed.

If you need to open the battery compartment, don't open it in a dusty or wet environment.

You should make sure that the battery cover is closed to ensure that dust and water cannot enter the battery compartment.

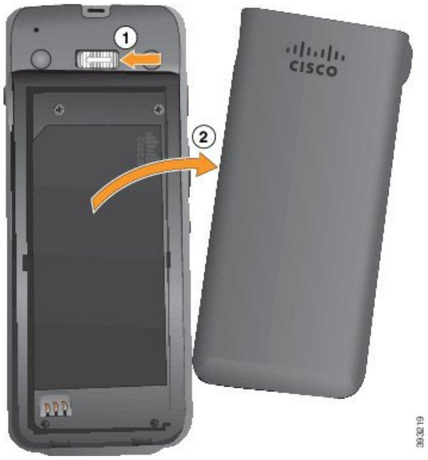
Note Dirt, oil, or other products can damage the gasket on the battery compartment cover, resulting in a poor seal. Every time you change the battery, inspect the gasket for damage. If the gasket is damaged, you can order a replacement cover.

Caution Phone life and functions could be compromised if:

- The battery is installed incorrectly.
- The battery cover is not closed properly.
- The rubber gasket on battery cover is poorly maintained.
- The rubber gasket on battery cover is damaged.
- The phone is dropped on a hard surface on a regular basis.

Procedure

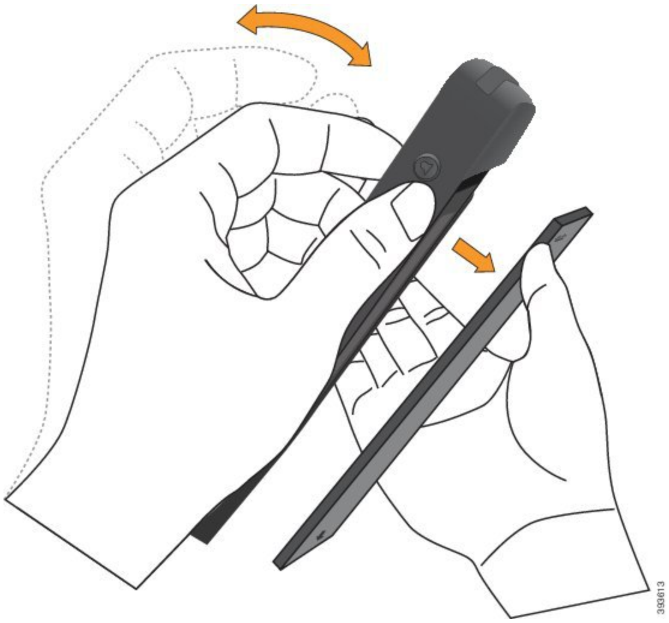
Step 1 Remove the cover from the battery compartment.



a) Push and hold the locking catch to the left to release the cover.
b) Use the tabs on the sides of the cover to lift the top of the cover and lift the cover up to unlock the bottom tabs .

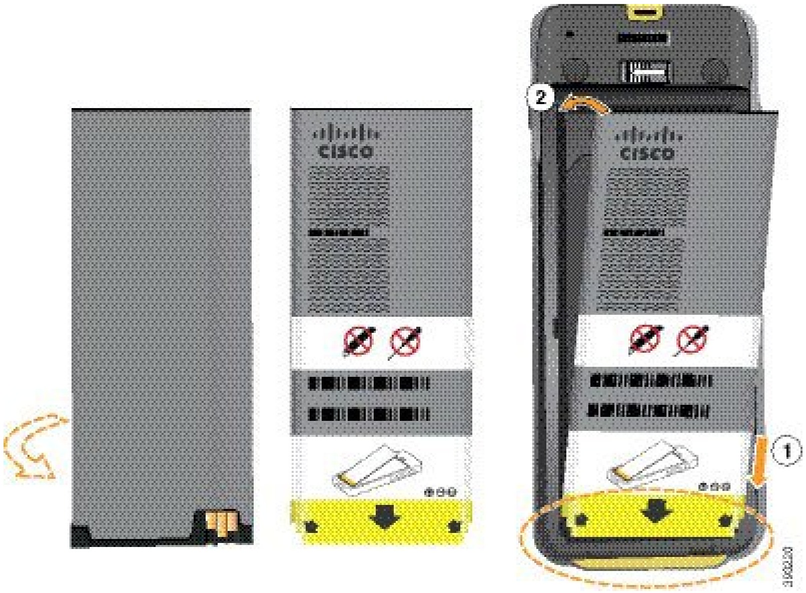
Step 2 Do one of these actions:

- If the battery has a pull tab, pull the tab away from the phone
- If the battery doesn't have a pull tabe, hold the phone in one hand with the screen towards the palm of your hand. Cup your other hand near the base of the phone. Shake the phone to make the battery fall into your hand.



Step 3 Install the battery.

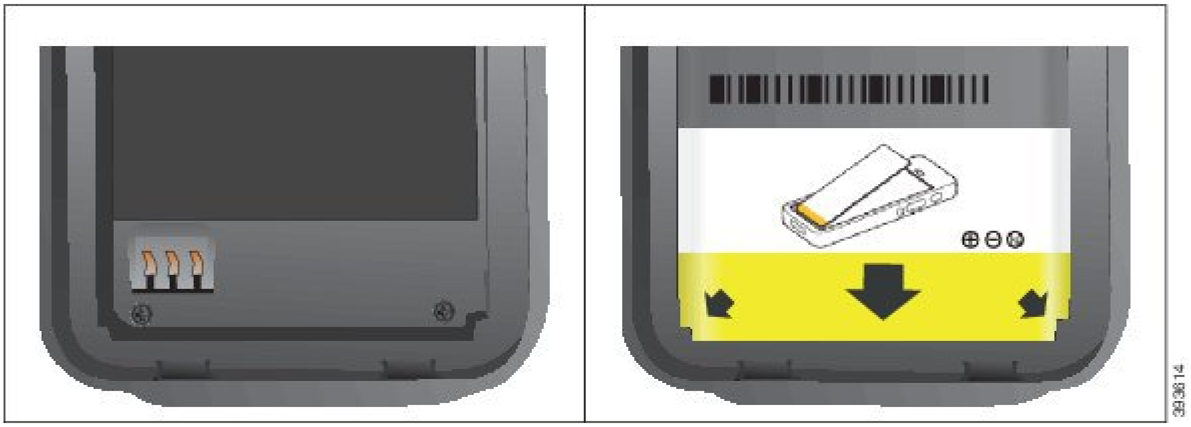
Caution If you install the battery incorrectly in the battery compartment, the battery and the battery compartment will be damaged.



The battery has metal contacts that must connect to the contacts in the battery compartment. The battery also has an arrow at the bottom and the Cisco logo at the top.

When the battery is correctly inserted, the logo and arrow are visible. The arrow points towards the connector on the base of the phone and the logo is close to the locking catch.

The battery compartment has small tabs in the bottom corners. The battery must slide under these tabs. The following graphic shows the battery compartment without and with the battery correctly installed.



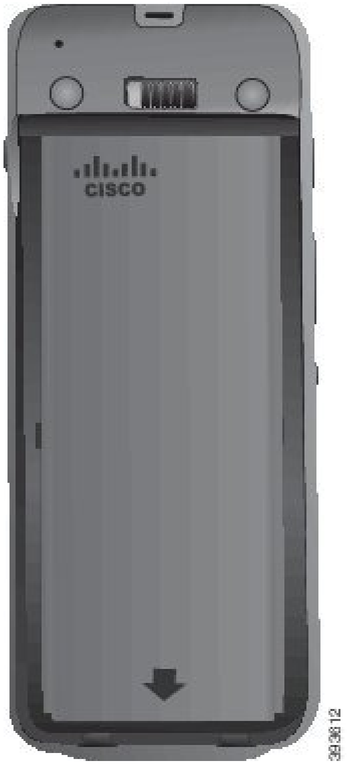
a) Hold the battery so that the lower edge is close to the bottom of the compartment. Make sure that the metal contacts on the phone and battery face each other. On the battery, the Cisco logo must be near the locking catch and the arrow must point to the base of the phone.

Caution Do not force the battery into the compartment or you will damage the compartment and the battery.

b) Slide the bottom of the battery under the tabs in the bottom of the battery compartment.

c) Press the battery into the battery compartment until it is flat in the compartment.

The following graphic shows a properly-installed battery.

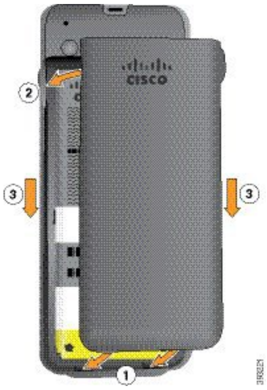


d) If the battery has a light plastic pull tab, the tab should be flat in the compartment.

Step 4 Inspect the gasket on the inside of the battery compartment cover and, if necessary, clean it with a cloth dampened with water.

Caution Do not use oil- or alcohol-based cleaners on the gasket. These cleaners will damage the gasket and void the phone warranty.

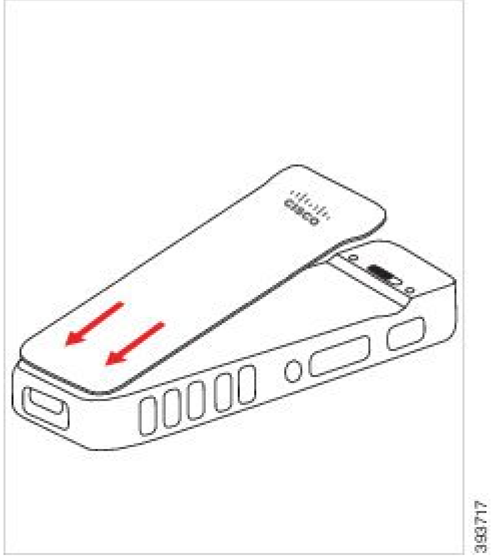
Step 5 Replace the cover to the battery compartment.



Caution When you close the battery cover, make sure that it is completely closed. Otherwise dust and water can enter the battery compartment.

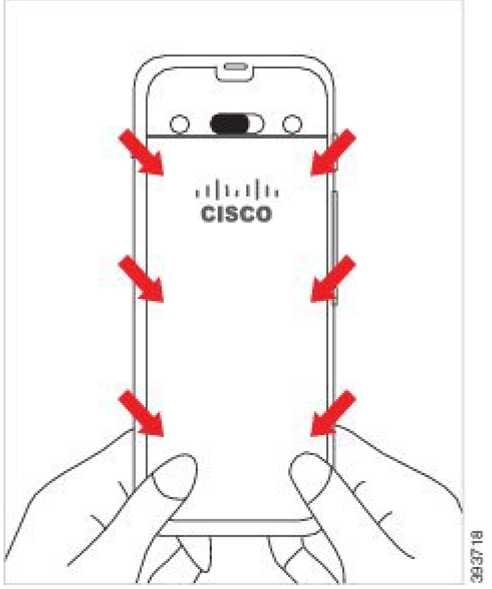
a) Align the tabs at the bottom of the cover into the notches on the phone.

The tabs slide into the phone.



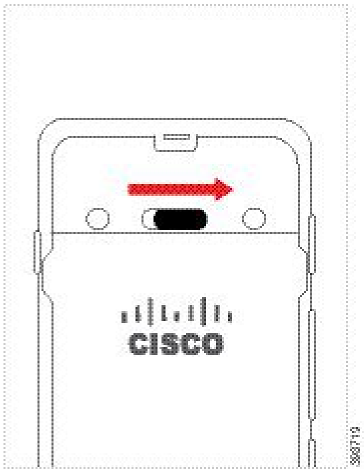
b) Press the cover firmly against the phone until it clicks in place. Press at the top, middle, and bottom of the cover on each side.

Press the cover firmly.



Caution Do not force the cover. If it doesn't click into place easily, remove the cover and check that the battery is inserted correctly.

c) Check that the cover is flush with the phone, then slide the lock to the right to lock the cover in place.



Replace the Cisco Wireless IP Phone 8821-EX Battery

Use this task for the Cisco Wireless IP Phone 8821-EX only. For the Cisco Wireless IP Phone 8821, see Replace the Cisco Wireless IP Phone 8821 Battery, on page 44.

If you have a spare battery, you can replace a depleted battery with a charged battery.

IP67 compliance mean that the phone is sealed from dust and water. When the phone leaves the factory, it is completely sealed.

⚠

Caution If you need to open the battery compartment, don't open it in a dusty or wet environment or in a hazardous location.

Don't open the compartment if the temperature is 0°C or less.

You should make sure that the battery cover is closed to ensure that dust and water cannot enter the battery compartment.

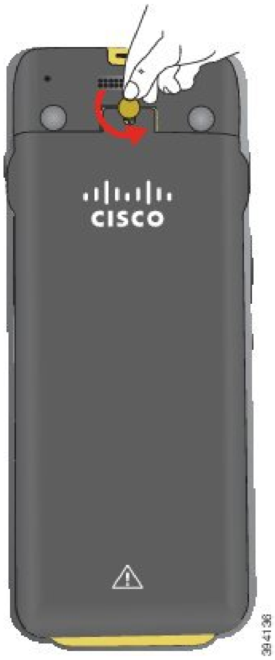
Note Dirt, oil, or other products can damage the gasket on the battery compartment cover, resulting in a poor seal. Every time you change the battery, inspect the gasket for damage. If the gasket is damaged, you can order a replacement cover.

Caution Phone life and functions could be compromised if:

- The battery is installed incorrectly.
- The battery cover is not closed properly.
- The rubber gasket on battery cover is poorly maintained.
- The rubber gasket on battery cover is damaged.
- The phone is dropped on a hard surface on a regular basis.

Procedure

Step 1 Use a coin to unscrew the battery cover and remove the cover from the battery compartment.



Caution Don't use a sharp object to unscrew the battery compartment door or to pry the battery door off the phone.

a) Use a coin to turn the screw and unlock the battery compartment.

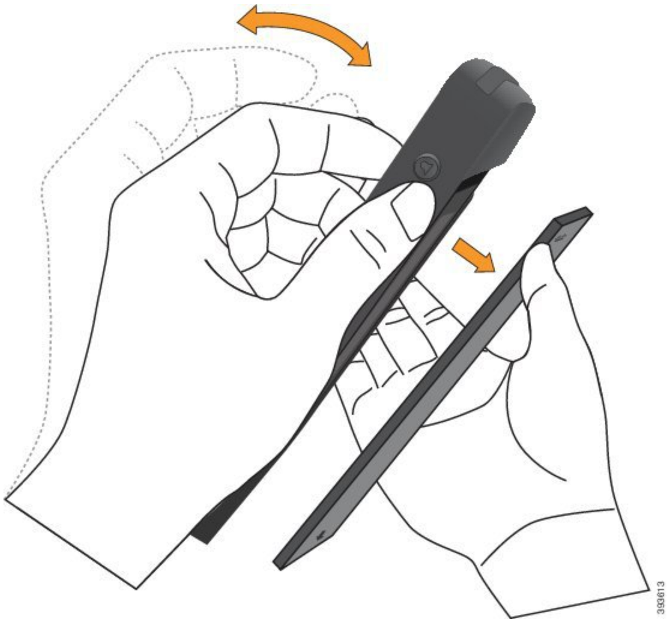
The screw remains in the cover.

b) Lift and remove the cover of the battery compartment with your fingers, *one corner at a time*.

Step 2 Do one of these actions:

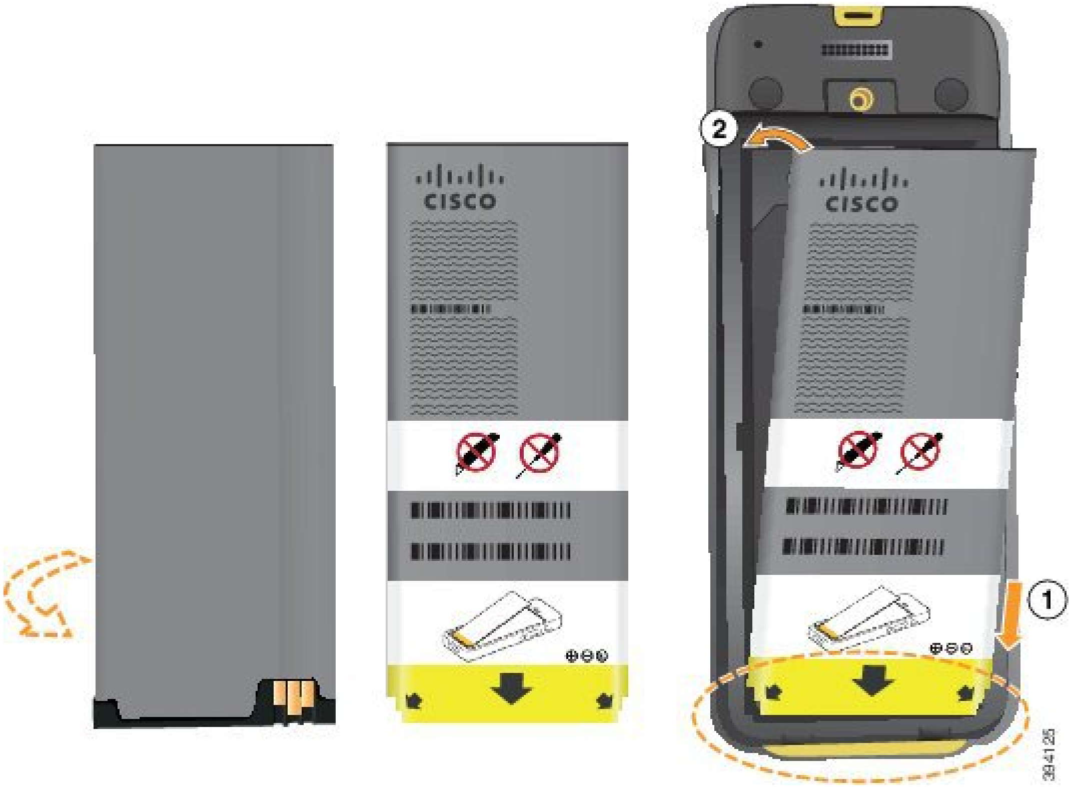
- If the battery has a pull tab, pull the tab away from the phone

- If the battery doesn't have a pull tabe, hold the phone in one hand with the screen towards the palm of your hand. Cup your other hand near the base of the phone. Shake the phone to make the battery fall into your hand.



Step 3 Install the battery.

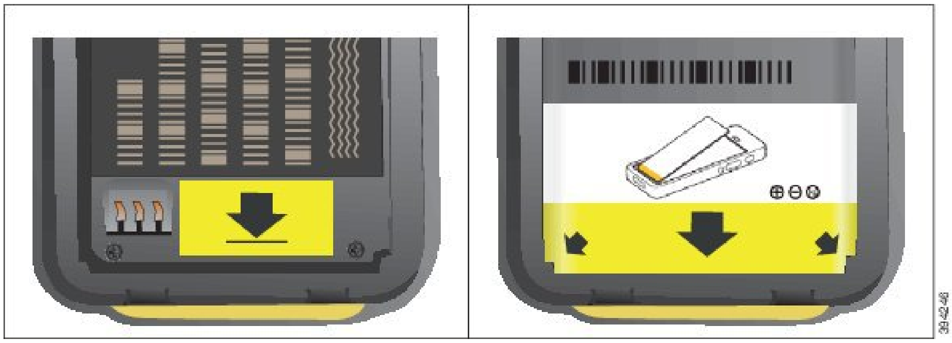
Caution If you install the battery incorrectly in the battery compartment, the battery and the battery compartment will be damaged.



The battery has metal contacts that must connect to the contacts in the battery compartment. The battery also has an arrow at the bottom and the Cisco logo at the top.

When the battery is correctly inserted, the logo and arrow are visible. The arrow points towards the connector on the base of the phone and the logo is close to the locking catch.

The battery compartment has small tabs in the bottom corners. The battery must slide under these tabs. The following graphic shows the battery compartment without and with the battery correctly installed.



a) Hold the battery so that the lower edge is close to the bottom of the compartment. Make sure that the metal contacts on the phone and battery face each other. On the battery, the Cisco logo must be near the locking catch and the arrow must point to the base of the phone.

Caution Do not force the battery into the compartment or you will damage the compartment and the battery.

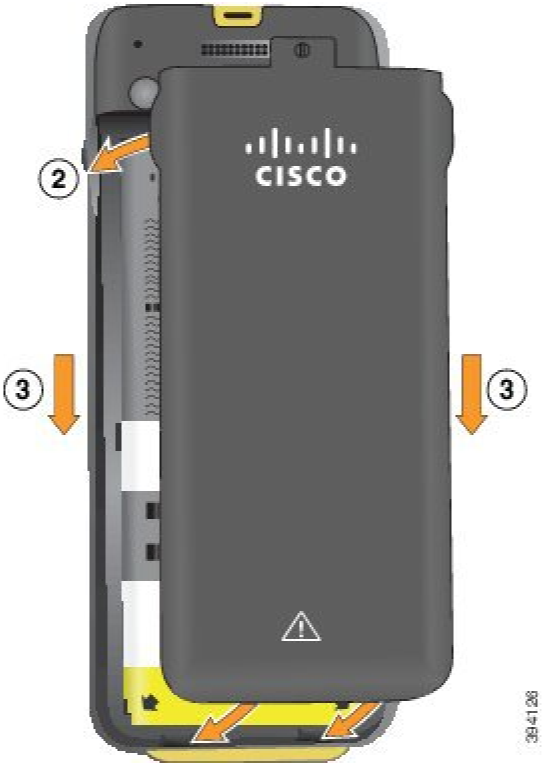
b) Slide the bottom of the battery under the tabs in the bottom of the battery compartment.

c) Press the battery into the battery compartment until it is flat in the compartment.

Step 4 Inspect the gasket on the inside of the battery compartment cover and, if necessary, clean it with a cloth dampened with water.

Caution Do not use oil- or alcohol-based cleaners on the gasket. These cleaners will damage the gasket and void the phone warranty.

Step 5 Replace the cover to the battery compartment.



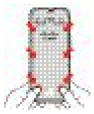
Caution When you close the battery cover, make sure that it is completely closed. Otherwise dust and water can enter the battery compartment.

a) Align the tabs at the bottom of the cover into the notches on the phone.

The tabs slide into the phone.

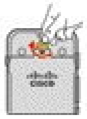
b) Press the cover firmly against the phone until it clicks in place.

Press at the top, middle, and bottom of the cover on each side.

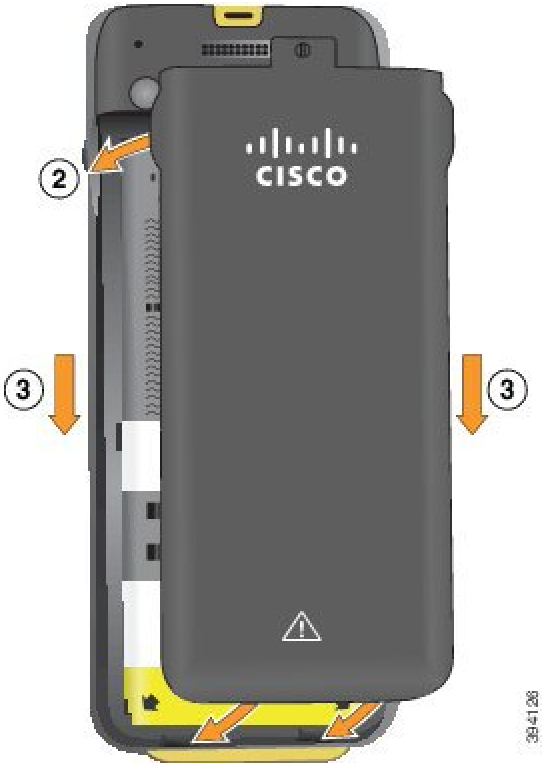


Caution Do not force the cover down. If it doesn't click into place easily, remove the cover and check that the battery is inserted correctly.

c) Check that the cover is flush with the phone, then use a coin to lock the cover in place.



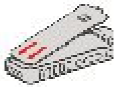
Step 6 Replace the cover to the battery compartment.



Caution When you close the battery cover, make sure that it is completely closed. Otherwise dust and water can enter the battery compartment.

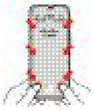
a) Align the tabs at the bottom of the cover into the notches on the phone.

The tabs slide into the phone.



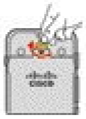
b) Press the cover firmly against the phone until it clicks in place.

Press at the top, middle, and bottom of the cover on each side.



Caution Do not force the cover down. If it doesn't click into place easily, remove the cover and check that the battery is inserted correctly.

c) Check that the cover is flush with the phone, then use a coin to screw the cover in place. The screw should be snug. Don't make it too tight.



Phone Battery Charging

You can charge the battery using any of the following options:

- USB cable—You can charge the phone with an AC power adapter or your computer.
- Desktop charger—You can use the phone and charge it at the same time.
- Multicharger—You can charge several phones at the same time.

Warning Explosion Hazard: Do not charge the phone battery in a potentially explosive atmosphere. Statement 431

The battery takes about 3 hours to charge in the AC power adapter, desktop charger, or multicharger. It takes about 6 hours to charge using the USB cable and your computer.

Spare Battery Charging

If you require longer talk times, you will find it useful to have a spare, charged battery. You can charge a spare battery in the desktop charger or multicharger.

Warning Explosion Hazard: Do not charge the spare battery in a potentially explosive atmosphere. Statement 431

The spare battery takes about 3 hours to charge in the desktop charger or multicharger.

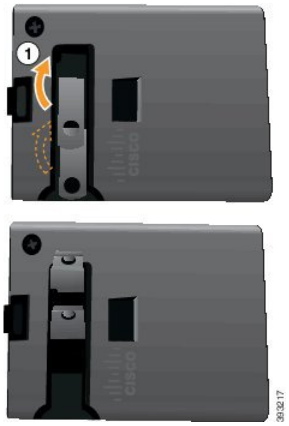
Prepare the Power Adapter

The power adapter for your phone is compact. Before you use the power adapter, you have to unfold the prongs. After you use the adapter, you can fold in the prongs.

The power adapter for your region may also require an additional clip to allow the adapter to be plugged into the electrical outlet.

Procedure

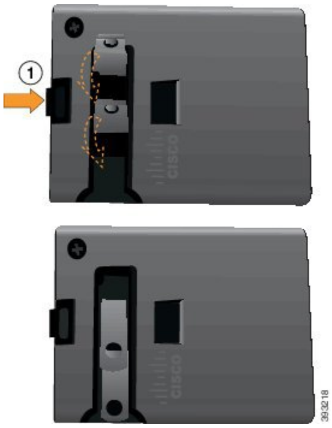
Step 1 Catch the edge of a prong with your finger and pull the prong up until it clicks into position.



Step 2 (Optional) Install the international power clip.

Step 3 (Optional) Before you close the adapter, remove the international power clip.

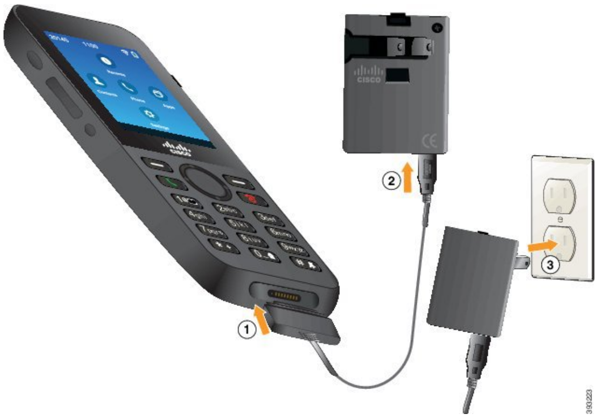
Step 4 (Optional) Hold the lever on the top of the adapter down and press the prongs down to close the adapter.



Charge the Battery with the AC Power Supply

You can charge your phone using an AC power supply. When you use the power supply to charge your phone, the battery can take up to 3 hours to fully charge.

The wide connector on the USB cable connects to the phone using magnets to hold it secure. It has pins that you need to align correctly. If you hold the phone so that the screen is towards you, the battery icon on the connector is visible.



Caution Do not charge the phone in a hazardous environment.

Do not charge the phone if it is wet.

Before you begin

You need the USB power cable supplied with your phone.

You need to prepare the power adapter for use as described in Prepare the Power Adapter, on page 55.

Procedure

Step 1 Plug the USB cable into the bottom of the phone with the pins aligned.

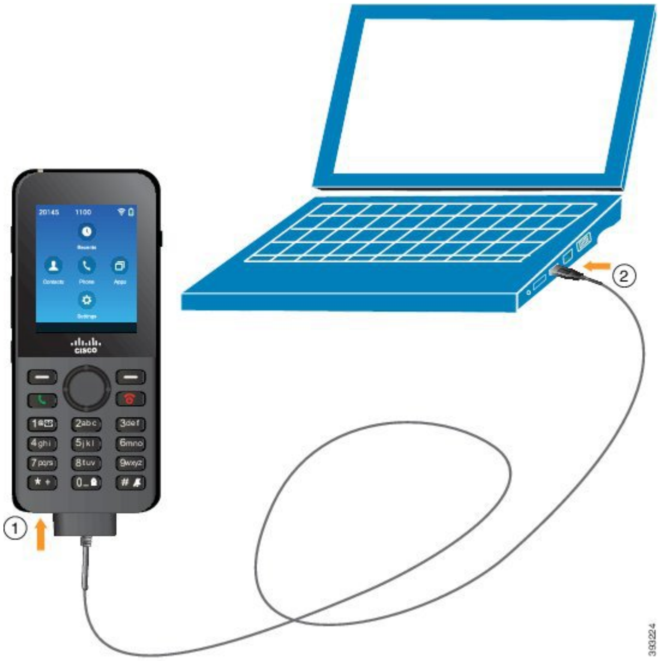
Step 2 Plug the USB cable into the power adapter.

Step 3 Plug the power adapter into the electrical outlet.

Charge the Battery with the USB Cable and a USB Port on Your Computer

You can charge your phone using your computer. When you use the computer to charge your phone, the battery can take up to 6 hours to fully charge.

The wide connector on the USB cable connects to the phone using magnets to hold it secure. It has pins that you need to align correctly. If you hold the phone so that the screen is towards you, the battery icon on the connector is visible.



Caution Do not charge the phone in a hazardous environment.

Do not charge the phone if it is wet.

Procedure

Step 1 Connect the long connecter of the USB cable to the bottom of the phone with the pins aligned.

Step 2 Plug the other end into the USB port in the computer.

Phone Configuration Tasks

When you set up a new phone, you connect it to your call control system and set up the phone features. This connection takes the following steps.

1. Gather information. You need the following information:
   - Wireless access point information: SSID, security type, security password or pin or key
   - MAC address of the phone
   - Directory number plan, to determine the DN to assign to the user
2. Set up the call control system:

   a. Ensure that your Cisco Unified Communications Manager has the latest firmware load and any required device packages.
   b. (Optional) Set up Wi-Fi profiles, Wi-Fi profile groups, phone button templates, softkey templates, and the common phone profile on the Cisco Unified Communications Manager.
   c. (Optional) Set up the Cisco Unified Communications Manager to automatically register phones.

3. If your Cisco Unified Communications Manager is not set up for automatic phone registration,
   a. Set up the new user.
   b. Add the new phone.
   c. Associated the new phone to the user.
   d. Enable the features that the user needs.

4. Set up the phone to connect to the call control system.

   After the phone is connected to the call control system, it should automatically update to the latest firmware load.

Related Topics

Cisco Unified Communications Manager Phone Configuration, on page 61
Configuration on the Phone, on page 87
Determine the MAC Address of the Phone, on page 61

CHAPTER 4

Cisco Unified Communications Manager Phone Configuration

Determine the MAC Address of the Phone

To add phones to the Cisco Unified Communications Manager, you must determine the MAC address of the phone.

Procedure

Perform one of the following actions:

- On the phone, access the **Settings** app, select **Phone information** > **Model information**, and look in the MAC address field.
- Remove the battery cover and battery from the phone, and look at the label.
- Display the phone web page and look at the MAC address in the **Device information** screen.
- If the phone has already been added to the Cisco Unified Communications Manager, access the Cisco Unified Communications Manager Administration application, select **Device** > **Phone**, search for the phone, and access the **Phone Configuration** window.

Related Topics

Access Web Page for Phone, on page 122

Access the Settings App, on page 88

Before You Register Wireless Phones

Before you register wireless phones with your Cisco Unified Communications Manager, you can set up profiles, groups, and templates. These can simplify the phone setup when you have common information for all phones or groups of phones.

- Wi-Fi profiles—you can create a profile for the Wi-Fi network connections.
- Wi-Fi profile groups—you can create a group of Wi-Fi profiles that the phones can use.
- Custom SIP Profile—the phone needs a special SIP Profile, instead of the standard SIP profiles.
- Phone button templates—you can assign lines and features in the **Phones** app. Use this if you have specific lines or features that you want all your users to access quickly. For example, you can set up a common speed dial number. Because the wireless phones have some special button requirements, Phone Button Templates, on page 65 will help you with this template.
- Softkey templates—you can set up the list of features that users see when they press the **More** ⋯ softkey. Because the wireless phones have fewer softkeys than desk phones, Phone Softkey Templates, on page 65 will help you with this template.
- Common phone profile—you can set up a profile for the wireless phone with the phone button and softkey templates, and then use the profile for all your wireless phones.

You can find detailed instructions about these profiles and templates in the *System Configuration Guide for Cisco Unified Communications Manager*.

Set Up a Wi-Fi Profile using Cisco Unified Communications Manager

You can configure a Wi-Fi profile and then assign the profile to the phones that support Wi-Fi. The profile contains the parameters required for phones to connect to the Cisco Unified Communications Manager with Wi-Fi. When you create and use a Wi-Fi profile, you or your users do not need to configure the wireless network for individual phones.

Wi-Fi profiles are supported on Cisco Unified Communications Manager Release 10.5(2) or later. EAP-FAST, PEAP-GTC, and PEAP-MSCHAPv2 are supported in Cisco Unified Communications Manager Release 10.0 and later. EAP-TLS is supported in Cisco Unified Communications Manager Release 11.0 and later.

A Wi-Fi profile enables you to prevent or limit changes to the Wi-Fi configuration on the phone by the user.

We recommend that you use a secure profile with TFTP encryption enabled to protect keys and passwords when you use a Wi-Fi profile.

When you set up the phones to use EAP-FAST, PEAP-MSCHAPv2, or PEAP-GTC authentication, your users need individual user ids and passwords to sign into the phone.

The phones support one server certificate per install method (manual, SCEP, or TFTP).

Procedure

Step 1 In the Cisco Unified Communications Administration, select **Device** > **Device Settings** > **Wireless LAN Profile**.

Step 2 Click **Add New**.

Step 3 In the **Wireless LAN Profile Information** section, set the parameters:

- **Name**—Enter a unique name for the Wi-Fi profile. This name displays on the phone.
- **Description**—Enter a description for the Wi-Fi profile to help you differentiate this profile from other Wi-Fi profiles.
- **User Modifiable**—Select an option:
  - **Allowed**—Indicates that the user can make changes to the Wi-Fi settings from their phone. This option is selected by default.
  - **Disallowed**—Indicates that the user cannot make any changes to the Wi-Fi settings on their phone.
  - **Restricted**—Indicates that the user can change the Wi-Fi username and password on their phone. But users are not allowed to make changes to other Wi-Fi settings on the phone.

Step 4 In the **Wireless Settings** section, set the parameters:

- **SSID (Network Name)**—Enter the network name available in the user environment to which the phone can be connected. This name is displayed under the available network list on the phone and the phone can connect to this wireless network.
- **Frequency Band**—Available options are Auto, 2.4 GHz, and 5 GHz. This field determines the frequency band that the wireless connection uses. If you select Auto, the phone attempts to use the 5 GHz band first and only uses the 2.4 GHz band when the 5 GHz is not available.

Step 5 In the **Authentications Settings** section, set the **Authentication Method** to one of these authentication methods: EAP-FAST, EAP-TLS, PEAP-MSCHAPv2, PEAP-GTC, PSK, WEP, and None.

After you set this field, you may see extra fields that you need to set.

- **User certificate**—Required for EAP-TLS authentication. Select **Manufacturing installed** or **User installed**. The phone requires a certificate to be installed, either automatically from the SCEP or manually from the administration page on the phone.
- **PSK passphrase**—Required for PSK authentication. Enter the 8- 63 character ASCII or 64 HEX character pass phrase.
- **WEP Key**—Required for WEP authentication. Enter the 40/102 or 64/128 ASCII or HEX WEP key.
  - 40/104 ASCII is 5 characters.
  - 64/128 ASCII is 13 characters.
  - 40/104 HEX is 10 characters.
  - 64/128 HEX is 26 characters.
- **Provide Shared Credentials**: Required for EAP-FAST, PEAP-MSCHAPv2, and PEAP-GTC authentication.
  - If the user manages the username and password, leave the **Username** and **Password** fields blank.
  - If all your users share the same username and password, you can input the information in the **Username** and **Password** fields.

- Enter a description in the **Password Description** field.

Note If you need to assign each user a unique username and password, you need to create a profile for each user.

Note The **Network Access Profile** field is not supported by the Cisco IP Phone 8821.

Step 6 Click **Save**.

What to do next

Apply the WLAN Profile Group to a device pool (**System** > **Device Pool**) or directly to the phone (**Device** > **Phone**).

Set Up a Wi-Fi Group using Cisco Unified Communications Manager

You can create a wireless LAN profile group and add any wireless LAN profile to this group. The profile group can then be assigned to the phone when you set up the phone.

If your users require access to more than one profile, then a profile group can speed up phone configuration. Up to four profiles can be added to the profile group and you list the profiles in priority order.

Procedure

Step 1 In Cisco Unified Communications Administration, select **Device** > **Device Settings** > **Wireless LAN Profile Group**.

You can also define a wireless LAN profile group from **System** > **Device Pool**.

Step 2 Click **Add New**.

Step 3 In the **Wireless LAN Profile Group Information** section, enter a group name and description.

Step 4 In the **Profiles for this Wireless LAN Profile Group** section, select an available profile from the **Available Profiles** list and move the selected profile to the **Selected Profiles** list.

Step 5 Click **Save**.

Set up a Wireless Phone SIP Profile

Cisco Unified Communication Manager has standard SIP profiles available. However, a custom SIP Profile for your wireless phones is the preferred profile.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, select **Device** > **Device Settings** > **SIP Profile**.

Step 2 Click **Find**.

Step 3 Click the **Copy** icon beside **Standard SIP Profile**.

Step 4 Set the name and description to `Custom 8821 SIP Profile`.

Step 5 Set these parameters.

- **Timer Register Delta (seconds)**—Set to 30 (default is 5).
- **Timer Keep Alive Expires (seconds)**—Set to 300 (default is 120).
- **Timer Subscribe Expires (seconds)**—Set to 300 (default is 120).
- **Timer Subscribe Delta (seconds)**—Set to 15 (default is 5).

Step 6 Click **Save**.

Phone Button Templates

You can assign lines and features to the wireless phones with a phone button template. Ideally, you set up the templates before you register the phones on the network. In this way, you can use a customized phone button template when you register the phone. But if you don't set up the template first, you can change the phones later.

The Cisco 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 dials. You can assign the following features to button positions:

- Service URL
- Privacy
- Speed dial

Use softkey features in the **More** menu to access other phone features, such as call park, call forward, redial, hold, resume, and conferencing.

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, see the *System Configuration Guide for Cisco Unified Communications Manager*.

Phone Softkey Templates

You can change the order of softkeys for the wireless phone with Cisco Unified Communications Manager Administration. Unlike other phones that have buttons for some functions, the wireless phone has two nonconfigurable softkeys. One of the softkeys is usually the **More** ⋯ softkey, and when you press **More**, you get a menu of appropriate actions.

When you configure a softkey template for the wireless phone, you configure the Cisco Unified Communications Manager softkeys and their sequence in the **More** menu only. The order of softkeys in the softkey template corresponds to the phone softkey list in the **More** menu. You can control the softkey display based on the call state.

You can copy the **Standard User** softkey template and set it up as your standard wireless phone softkey template. You can then copy your standard wireless phone softkey template if some of your users have specific requirements.

For example, if most of your users want the **Hold** softkey as the first entry in the **More** menu, and the rest of the users want **Transfer** in the first entry:

- Set up your standard wireless softkey template with the **Hold** softkey as the first softkey when the phone is in the connected state.
- Copy the standard wireless softkey template, give it a new name and set the first softkey to be **Transfer** when the phone is in the connected state.
- When you set up your user and phones, you can assign the appropriate softkey template.

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 templates support up to 16 softkeys for applications.

For more information, see the *System Configuration Guide for Cisco Unified Communications Manager*.

Bulk Deployment Utility

The Bulk Deployment Utility (BDU) for the Cisco Wireless IP Phone 8821 enables you to quickly provision and deploy wireless phones when unique 802.1x accounts are used with EAP-FAST, PEAP-GTC, or PEAP-MS-CHAPv2, or if a common set of credentials are used by all phones (for example, WPA2-PSK or a common 802.1x account). You can also use the BDU to support the phones after they are deployed. The BDU does not support certificate provisioning.

The BDU requires Firmware Release 11.0(3)SR4 or later on the phones.

Note This version of the BDU is not the same as the BDU for the Cisco Unified Wireless IP Phone 792x Series.

You download the BDU from this location:

https://software.cisco.com/download/type.html?mdfid=286308995&flowid=80142

For more information, see the *Bulk Deployment Utility Guide for Cisco Wireless Phone 8821 and 8821-EX* that is associated with the BDU software.

Manual Phone Registration

When a new phone is added to your network, manual phone registration means that you need to configure the phone in your call control system. The configuration includes the directory number, information about the user, and the phone profile.

After you configure the phone in the call control system, you configure the phone to connect to the call control system.

Related Topics

Manually Set Up the Phone Network from the Settings Menu , on page 87

Add a New Phone

Before the phone can be used, you add it to the Cisco Unified Communications Manager and assign it to a user. If you do not set up Wi-Fi profile groups, you or your user need to set up the Wi-Fi network on the phone.

Before you begin

You need the following files installed on the Cisco Unified Communications Manager:

- Latest phone firmware load
- Latest Cisco Unified Communications Manager Device Pack to support the phone

You need the MAC address of the phone.

Your user must be configured in the system.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, select **Device** > **Phone**.

Step 2 Click **Add New**.

Step 3 Select **Cisco 8821**.

If **Cisco 8821** does not appear, the Cisco Unified Communications Manager Device Pack to support the phone is not installed on the server.

Step 4 Click **Next**.

Step 5 Set the phone information.

Required fields are marked with an asterisk (*), although most take the default settings. The fields that need specific entries are:

- MAC address—Enter the MAC address of the phone. You can enter the address with lowercase letters.
- Description—Set this field to something meaningful; for example, the user's name.
- Device pool—Set this field for the appropriate pool of phones.
- Phone Button Template—Select **Standard 8821 SIP**.
- Owner User ID—Select the user's ID.
- Device security profile—Select **Cisco 8821 Standard SIP Non Secure Profile**.
- SIP profile—Select **Custom 8821 SIP Profile**. For more information, see Set up a Wireless Phone SIP Profile, on page 64.

Step 6 (Optional) In the **Wireless LAN Profile Group** field, select the wireless LAN profile group if the profile is not associated with a device pool. For more information, see Set Up a Wi-Fi Profile using Cisco Unified Communications Manager, on page 62.

Step 7 Click **Save**.

Step 8 Click **OK**.

Step 9 Click **Apply config**.

Step 10 Click **OK**.

Step 11 Click **Line[1] — Add a new DN**.

Step 12 Enter a DN.

Step 13 Click **Save** and then click **Save** again.

Step 14 In the **Related links** field, select **Configure Device** and click **Go**.

Step 15 Click **Save** and click **OK**.

Step 16 Click **Apply config** and click **OK**.

What to do next

If you do not use a Wi-Fi profile group, then you need to configure the wireless network on the phone.

Automatic Phone Registration

If your Cisco Unified Communications Manager is set up to automatically register new phones, you can get new phones working quickly. You need to set up the phone to connect to your Cisco Unified Communications Manager. The new phones are assigned DNs and profiles based on the phone type.

To support autoregistration, you need to set up profiles for the phone models or use the standard profiles.

For more information on autoregistration, see the Cisco Unified Communications Manager documentation.

Related Topics

Add the Phone to the Wi-Fi Network, on page 89

Phone Feature Configuration

You can set up phones to have a variety of features, based on the needs of your users. You can apply features to all phones, a group of phones, or to individual phones.

When you set up features, the Cisco Unified Communications Manager Administration window displays information that is applicable to all phones and information that is applicable to the phone model. The information that is specific to the phone model is in the Product Specific Configuration Layout area of the window.

For information on the fields applicable to all phone models, see the Cisco Unified Communications Manager documentation.

When you set a field, the window that you set the field in is important because there is a precedence to the windows. The precedence order is:

1. Individual phones (highest precedence)
2. Group of phones
3. All phones (lowest precedence)

For example, if you don't want a specific set of users to access the phone Web pages, but the rest of your users can access the pages, you:

1. Enable access to the phone web pages for all users.
2. Disable access to the phone web pages for each individual user, or set up a user group and disable access to the phone web pages for the group of users.
3. If a specific user in the user group did need access to the phone web pages, you could enable it for that particular user.

Set Up Phone Features for all Phones

Procedure

Step 1 Sign into Cisco Unified Communications Manager Administration as an administrator.

Step 2 Select **Device** > **Device Settings** > **Common Phone Profile**

Step 3 Locate the phones.

Step 4 Navigate to the Product Specific Configuration Layout pane and set the fields.

Step 5 Check the **Override Enterprise Settings** check box for any changed fields.

Step 6 Click **Save**.

Step 7 Click **Apply Config**.

Step 8 Restart the phones.

Related Topics

Product Specific Configuration Fields, on page 70

Set Up Phone Features for a Group of Phones

Procedure

Step 1 Sign into Cisco Unified Communications Manager Administration as an administrator.

Step 2 Select **Device** > **Device Settings** > **Common Phone Profile**

Step 3 Locate the group of users.

Step 4 Navigate to the Product Specific Configuration Layout pane and set the fields.

Step 5 Check the **Override Enterprise Settings** check box for any changed fields.

Step 6 Click **Save**.

Step 7 Click **Apply Config**.

Step 8 Restart the phones.

Related Topics

Product Specific Configuration Fields, on page 70

Set Up Phone Features for a Single Phone

Procedure

Step 1 Sign into Cisco Unified Communications Manager Administration as an administrator.

Step 2 Select **Device** > **Phone**

Step 3 Locate the phone associated with the user.

Step 4 Navigate to the Product Specific Configuration Layout pane and set the fields.

Step 5 Check the **Override Common Settings** check box for any changed fields.

Step 6 Click **Save**.

Step 7 Click **Apply Config**.

Step 8 Restart the phone.

Related Topics

Product Specific Configuration Fields, on page 70

Product Specific Configuration Fields

The following table describes the fields in the Product Specific Configuration Layout pane.

Table 6: Product Specific Configuration Fields

Field Name	Field Type Or Choices	Default	Description
Disable Speakerphone	Checkbox	Unchecked	Turns off the speakerphone capability of the handset. See Note 1.
Disable Speakerphone and Headset	Checkbox	Unchecked	Turns off the speakerphone and headset capability of the handset. See Note 1.
Settings Access	Disabled Enabled Restricted	Enabled	Enables, disables, or restricts access to local configuration settings in the Settings app. With restricted access, the Phone Settings, Bluetooth, and Phone Information menus can be accessed. Some settings in the Wi-Fi menu are also accessible. With disabled access, the Settings menu does not display any options.
Web Access	Disabled Enabled	Disabled	Enables or disables access to the phone web pages through a web browser.

Field Name	Field Type Or Choices	Default	Description
HTTPS Server	HTTP and HTTPS enabled HTTPS only	HTTP and HTTPS enabled	Controls the type of communication to the phone. If you select HTTPS only, the phone communication is more secure.
Disable TLS 1.0 and TLS 1.1 for Web Access	Disabled Enabled	Disabled	Controls the use of TLS 1.2 for a web server connection. • Disabled—A phone configured for TLS1.0, TLS 1.1, or TLS1.2 can function as an HTTPS server. • Enabled—Only a phone configured for TLS1.2 can function as an HTTPS server.
Web Admin	Disabled Enabled	Disabled	Enables or disables administrator access to the phone web pages through a web browser
Admin Password	String of 8–127 characters		Defines the administrator password when you access the phone web pages as an administrator.
Bluetooth	Disabled Enabled	Enabled	Enables or disables the Bluetooth option on the phone. If disabled, the user cannot enable Bluetooth on the phone.
Out-of-Range Alert	Disabled Beep once Beep every 10 seconds Beep every 30 seconds Beep every 60 seconds	Disabled	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	Continuous	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.
Application URL	String of up to 256 characters		Specifies the URL that the phone uses to contact application services, including Push To Talk.

Field Name	Field Type Or Choices	Default	Description
Application Button Activation Timer	Disabled 1 second 2 seconds 3 seconds 4 seconds 5 seconds	Disabled	Specifies the amount of time that the user must hold the Application button to activate the Application URL.
Application Button Priority	Low Medium High	Low	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. When the priority is high, the keypad locked and the screen dark, pressing the application button turns on the phone screen. The user presses the button a second time to perform the application button function.
Emergency Numbers	String of up to 16 characters, comma separated, no spaces		Sets the list of emergency numbers that the users see when they try to dial without signing in. Example: 911,411
Dialing Mode	On-hook Dialing Off-hook Dialing	On-hook Dialing	Sets the default dialing mode for the phones.
Power Off in Multicharger	Disabled Enabled	Disabled	When disabled, the phone doesn't power off when placed in the multicharger. When enabled, the phone powers off when placed in the multicharger.
Background Image	String up to 64 characters		Sets the background image that all users see. If you set a background image, the user cannot change the phone to another image.
Home Screen	Application View Line View	Application View	Sets the home screen to either the Application View or the Line View. Set the phone to use Line View for users that use multiple lines, speed dials, or make many calls.

Field Name	Field Type Or Choices	Default	Description
Voicemail Access	Disabled Enabled	Enabled	Controls access to voicemail.
Applications Access	Disabled Enabled	Enabled	Controls access to the Applications menu.
Recording Tone	Disabled Enabled	Disabled	Controls the playing of the tone when a user is recording a call
Recording Tone Local Volume	Integer 0–100	100	Controls the volume of the recording tone to the local user.
Recording Tone Remote Volume	Integer 0–100	50	Controls the volume of the recording tone to the remote user.
Recording Tone Duration	Integer 1–3000 milliseconds		Controls the duration of the recording tone.
Remote Log	Disabled Enabled	Disabled	Controls the ability to capture logs remotely.
Log Profile	Default Preset Telephony	Preset	Specifies the predefined logging profile.
Log Server	String of up to 256 characters		Identifies the IPv4 log server.
Cisco Discovery Protocol (CDP)	Disabled Enabled	Enabled	Controls Cisco Discovery Protocol on the phone.
SSH Access	Disabled Enabled	Disabled	Controls the access to the SSH daemon through port 22. Leaving port 22 open leaves the phone vulnerable to Denial of Service (DoS) attacks.
Ring Locale	Default Japan	Default	Controls the ringing pattern.
TLS Resumption Timer	Integer 0–3600 seconds	3600	Controls the ability to resume a TLS session without repeating the entire TLS authentication process. If the field is set to 0, then the TLS session resumption is disabled.
Record Call Log from Shared Line	Disabled Enabled	Disabled	Specifies whether to record call log from a shared line.

Field Name	Field Type Or Choices	Default	Description
Minimum Ring Volume	Silent Volume level 1–15	Silent	Controls the minimum ring volume for the phone.
Load Server	String of up to 256 characters		Identifies the alternate IPv4 server that the phone uses to obtain firmware loads and upgrades.
WLAN SCEP Server	String of up to 256 characters		Specifies the SCEP Server that the phone uses to obtain certificates for WLAN authentication. Enter the hostname or the IP address (using standard IP addressing format) of the server.
WLAN Root CA Fingerprint (SHA256 or SHA1)	String of up to 95 characters		Specifies the SHA256 or SHA1 fingerprint of the Root CA to use for validation during the SCEP process when issuing certificates for WLAN authentication. We recommend that you use the SHA256 fingerprint, which can be obtained via OpenSSL (e.g. openssl x509 -in rootca.cer -noout -sha256 -fingerprint) or using a Web Browser to inspect the certificate details. Enter the 64 hexadecimal character value for the SHA256 fingerprint or the 40 hexadecimal character value for the SHA1 fingerprint with a common separator (colon, dash, period, space) or without a separator. If using a separator, then the separator should be consistently placed after every 2, 4, 8, 16, or 32 hexadecimal characters for a SHA256 fingerprint or every 2, 4, or 8 hexadecimal characters for a SHA1 fingerprint.
Console Access	Disabled Enabled	Disabled	Specifies whether the serial console is enabled or disabled.
Gratuitous ARP	Disabled, Enabled	Disabled	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.
Show All Calls on Primary Line	Disabled Enabled	Disabled	Specifies is all calls presented to this phone will be shown on the primary line or not.

Field Name	Field Type Or Choices	Default	Description
Advertise G.722 and iSAC Codecs	Use System Default Disabled Enabled	Use System Default	Indicates whether the phone advertises the G.722 and iSAC codecs to the Cisco Unified Communications Manager. • 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. For more information, see Note 2.
Revert to All Calls	Disabled Enabled	Disabled	Specifies whether the phone will revert to All Calls after any call ends or not if the call is on a filter other than Primary line, All Calls, or Alerting Calls.
DF bit	0 1	0	Controls how network packets are sent. Packets can be sent in chunks (fragments) of various sizes. When the DF bit is set to 1 in the packet header, the network payload does not fragment when going through network devices, such as switches and routers. Removing fragmenting avoids incorrect parsing on the receiving side, but results in slightly slower speeds. The DF bit setting does not apply to ICMP, VPN, VXC VPN, or DHCP traffic.
Lowest Alerting Line State Priority	Disabled Enabled	Disabled	Specifies the alert state when using shared lines. When disabled and there is an incoming call alerting on the shared line, the LED/Line state icon reflects the alerting state instead of Remote-In-Use. When enabled, the user sees the Remote-In-Use icon when there is call alerting on the shared line.
Divert Alerting Call	Disabled Enabled	Enabled	Controls the display of the **Decline** softkey. • Disabled: the **Decline** softkey doesn't display when there is an incoming call. The user can't divert or dismiss the incoming call. • Enabled: the **Decline** softkey displays when there is an incoming call. The user can decline the call.

Field Name	Field Type Or Choices	Default	Description
Allow Vibrate URI When On Call	Disabled Enabled	Disabled	Controls if the Vibrate URI command from an XSI message is allowed when the phone is active on a call. • Disabled: The handset won't vibrate. • Enabled: The handset will vibrate.
Customer support upload URL	String of up to 256 characters		Identifies the location that the phones use to upload problem reporting tool (PRT) output files.

Note

1. If you change a user's audio path while they are in the Push to Talk session, the user needs to end the current session and restart to get the correct audio path selection.
2. Codec negotiation involves two steps:
   a. The phone must advertise the supported codec to the Cisco Unified Communications Manager (not all endpoints support the same set of codecs).
   b. 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.

Set Up Services

You can provide your users with special phone services. These services are XML applications that enable the display of interactive content with text and graphics on the phone. Examples of services include Push to Talk, directories, stock quotes, and weather reports. Some services, such as Push to Talk, can use the configurable **Applications** button that is located on the side of the phone.

Cisco does not provide any applications but you can create your own custom applications. For more information, see the *Cisco Unified IP Phone Service Application Development Notes*, located here: https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-programming-reference-guides-list.html.

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

- You use Cisco Unified Communications Manager Administration to configure the available services.
- You give information to your users about the services available. See Self Care Portal Overview, on page 79 for a summary of the information that you must provide to your users.
- The user subscribes to services using the Self Care portal.

These references will help you understand services:

- “Configure Cisco Unified IP Phone Services” in the *System Configuration Guide for Cisco Unified Communications Manager*

- "Extension Mobility" in the *Feature Configuration Guide for Cisco Unified Communications Manager*

Before you begin

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.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Device** > **Device Settings** > **Phone Services**.

Step 2 Set up the services.

Step 3 Verify that your users have access to the Self Care portal.

Problem Report Tool

Users submit problem reports to you with the Problem Report Tool.

Note The Problem Report Tool logs are required by Cisco TAC when troubleshooting problems. The logs are cleared if you restart the phone. Collect the logs before you restart the phones.

To issue a problem report, users access the Problem Report Tool and provide the date and time that the problem occurred, and a description of the problem.

You must add a server address to the **Customer Support Upload URL** field on Cisco Unified Communications Manager.

Configure a Customer Support Upload URL

You must use a server with an upload script to receive PRT files. The PRT uses an HTTP POST mechanism, with the following parameters included in the upload (utilizing multipart MIME encoding):

- devicename (example: "SEP001122334455")
- serialno (example: "FCH12345ABC")
- username (the username configured in Cisco Unified Communications Manager, the device owner)
- prt_file (example: "probrep-20141021-162840.tar.gz")

A sample script is shown below. This script is provided for reference only. Cisco does not provide support for the upload script installed on a customer's server.

```
<?php

// NOTE: you may need to edit your php.ini file to allow larger
// size file uploads to work.
// Modify the setting for upload_max_filesize
// I used:  upload_max_filesize = 20M

// Retrieve the name of the uploaded file
$filename = basename($_FILES['prt_file']['name']);
```

```
// Get rid of quotes around the device name, serial number and username if they exist
$devicename = $_POST['devicename'];
$devicename = trim($devicename, "'\"");

$serialno = $_POST['serialno'];
$serialno = trim($serialno, "'\"");

$username = $_POST['username'];
$username = trim($username, "'\"");

// where to put the file
$fullfilename = "/var/prtuploads/".$filename;

// If the file upload is unsuccessful, return a 500 error and
// inform the user to try again

if(!move_uploaded_file($_FILES['prt_file']['tmp_name'], $fullfilename)) {
        header("HTTP/1.0 500 Internal Server Error");
        die("Error: You must select a file to upload.");
}

?>
```

Procedure

Step 1 Set up a server that can run your PRT upload script.

Step 2 Write a script that can handle the parameters listed above, or edit the provided sample script to suit your needs.

Step 3 Upload your script to your server.

Step 4 In Cisco Unified Communications Manager, go to the Product Specific Configuration Layout area of the individual device configuration window, Common Phone Profile window, or Enterprise Phone Configuration window.

Step 5 Check **Customer support upload URL** and enter your upload server URL.

Example:

http://example.com/prtscript.php

Step 6 Save your changes.

Remote Problem Report Creation with XSI

You can request a PRT with the X/Open System Interface (XSI) CiscoIPPhoneExecute object. For more information, see the *Cisco Unified IP Phone Services Application Development Notes for Cisco Unified Communications Manager and Multiplatform Phones*.

Corporate and Personal Directories Setup

You can make it easy for your users to contact coworkers using a corporate directory.

You can also enable users to create personal directories. Each individual user has a personal directory, which they can access from any device.

The corporate and personal directories are set up in the Cisco Unified Communications Manager.

Corporate Directory Setup

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

Cisco Unified Communications Manager uses a Lightweight Directory Access Protocol (LDAP) directory to store authentication and authorization information about users of Cisco Unified Communications Manager applications that interface with Cisco Unified Communications Manager. Authentication establishes user rights to access the system. Authorization identifies the telephony resources that a user is permitted to use, such as a specific phone extension.

For more information, see the documentation for your particular Cisco Unified Communications Manager release.

After you complete the LDAP directory configuration, users can use the Corporate Directory service on their phone to look up users in the corporate directory.

Personal Directory Setup

The Personal Directory allows a user to store a set of personal numbers.

Personal Directory consists of the following features:

- Personal Address Book (PAB)
- Speed Dials

Users can use these methods to access Personal Directory features:

- From a web browser—Users can access the PAB and Speed Dials features from the Cisco Unified Communications Self Care Portal.
- From the Cisco IP Phone—Choose **Contacts** to search the corporate directory or the user personal directory.

To configure Personal Directory from a web browser, users must access their Self Care Portal. You must provide users with a URL and sign-in information.

Self Care Portal Overview

From the Cisco Unified Communications Self Care Portal, users can customize and control phone features and settings.

As the administrator, you control access to the Self Care Portal. You must also provide information to your users so that they can access the Self Care Portal.

Before a user can access the Cisco Unified Communications Self Care Portal, you must use Cisco Unified Communications Manager Administration to add the user to a standard Cisco Unified Communications Manager End User group.

You must provide end users with the following information about the Self Care Portal:

- The URL to access the application. This URL is:

`https://<server_name:portnumber>/ucmuser/`, where server_name is the host on which the web server is installed and portnumber is the port number on that host.

- A user ID and default password to access the application.
- An overview of the tasks that users can accomplish with the portal.

These settings correspond to the values that you entered when you added the user to Cisco Unified Communications Manager.

For more information, see the documentation for your particular Cisco Unified Communications Manager release.

Set Up User Access to the Self Care Portal

Before a user can access the Self Care Portal, you need to authorize the access.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, select **User Management** > **End User**.

Step 2 Search for the user.

Step 3 Click the user ID link.

Step 4 Ensure that the user has a password and PIN configured.

Step 5 In the Permission Information section, ensure that the Groups list includes **Standard CCM End Users**.

Step 6 Select **Save**.

Customize the Self Care Portal Display

Most options display on the Self Care Portal. However, you must set the following options by using Enterprise Parameters Configuration settings in Cisco Unified Communications Manager Administration:

- Show Ring Settings
- Show Line Label Settings

Note The settings apply to all Self Care Portal pages at your site.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, select **System** > **Enterprise Parameters**.

Step 2 In the Self Care Portal area, set the **Self Care Portal Default Server** field.

Step 3 Enable or disable the parameters that the users can access in the portal.

Step 4 Select **Save**.

Custom Wallpaper and Ringtones

You can add custom wallpaper and ringtones to the phones. For example, you might want a wallpaper with your corporate logo.

Custom Phone Rings

The phone ships with three ring tones that are implemented in hardware: Sunshine, Chirp, Chirp1.

Cisco Unified Communications Manager also provides a default set of additional phone ring sounds that are implemented in software as pulse code modulation (PCM) files. The PCM files, along with an XML file (named Ringlist-wb.xml) that describes the ring list options that are available at your site, exist in the TFTP directory on each Cisco Unified Communications Manager server.

Attention All file names are case sensitive. If you use Ringlist-wb.xml for the file name, the phone will not apply your changes.

For more information, see the "Custom Phone Rings and Backgrounds" chapter, Feature Configuration Guide for Cisco Unified Communications Manager for Cisco Unified Communications Manager release 12.0(1) or later.

Set Up Custom Phone Rings

Procedure

Step 1 Create a PCM file for each custom ring (one ring per file). Ensure the PCM files comply with the format guidelines that are listed in Custom Ring File Formats, on page 81.

Step 2 Upload the new PCM files that you created to the Cisco TFTP server for each Cisco Unified Communications Manager in your cluster. For more information, see the documentation for your particular Cisco Unified Communications Manager release.

Step 3 Use a text editor to edit the Ringlist-wb.xml file. See Custom Ring File Formats, on page 81 for information about how to format this file and for a sample Ringlist-wb.xml file.

Step 4 Save your modifications and close the file.

Step 5 To cache the new file, stop and start the TFTP service by using Cisco Unified Serviceability or disable and reenable the “Enable Caching of Constant and Bin Files at Startup” TFTP service parameter, located in the Advanced Service Parameters area.

Custom Ring File Formats

The Ringlist-wb.xml file defines an XML object that contains a list of phone ring types. This file includes up to 50 ring types. Each ring type contains a pointer to the PCM file that is used for that ring type and the text that appears on the Ring Type menu on a phone for that ring. The Cisco TFTP server for each Cisco Unified Communications Manager contains this file.

The CiscoIPPhoneRinglist XML object uses the following simple tag set to describe the information:

```
<CiscoIPPhoneRingList>
   <Ring>
      <DisplayName/>
      <FileName/>
   </Ring>
</CiscoIPPhoneRingList>
```

The following characteristics apply to the definition names. You must include the required DisplayName and FileName for each phone ring type.

- DisplayName specifies the name of the custom ring for the associated PCM file that displays on the Ring Type menu of the phone.
- FileName specifies the name of the PCM file for the custom ring to associate with DisplayName.

Note The DisplayName and FileName fields must not exceed 25 characters in length.

This example shows a Ringlist-wb.xml file that defines two phone ring types:

```
<CiscoIPPhoneRingList>
   <Ring>
      <DisplayName>Analog Synth 1</DisplayName>
      <FileName>Analog1.rwb</FileName>
   </Ring>
   <Ring>
      <DisplayName>Analog Synth 2</DisplayName>
      <FileName>Analog2.rwb</FileName>
   </Ring>
</CiscoIPPhoneRingList>
```

The PCM files for the rings must meet the following requirements for proper playback on the phones:

- Raw PCM (no header)
- 8000 samples per second
- 8 bits per sample
- Mu-law compression
- Maximum ring size = 16080 samples
- Minimum ring size = 240 samples
- Number of samples in the ring = multiple of 240.
- Ring start and end at zero crossing.

To create PCM files for custom phone rings, use any standard audio editing package that supports these file format requirements.

Custom Background Images

You can provide users with a choice of background images (or wallpaper) for the LCD screen on their phones. Users can select a background image by accessing the **Settings** app and choosing **Phone settings** > **Display** > **Wallpaper** on the phone.

The image choices that users see come from PNG images and an XML file (called List.xml) that are stored on the TFTP server that the phone uses. By storing your own PNG files and editing the XML file on the TFTP server, you can designate the background images from which users can choose. In this way, you can provide custom images, such as your company logo.

Note The dimensions for the PNG and List.xml images must be within 240x320x24.

If you create your own custom wallpaper, you must make sure that it will display correctly on the wireless phone. The phone uses white letters, so wallpapers with white or light-colored areas are not suitable.

Attention All file names are case sensitive. If you use list.xml for the file name, the phone will not apply your changes.

You can disable the option for users to select a background image. To do this, you uncheck the **Enable End User Access to Phone Background Image Setting** check box from the **Common Phone Profile Configuration** window in Cisco Unified Communications Manager Administration (**Device** > **Device Settings** > **Common Phone Profile**). When this check box is unchecked, the wallpaper menu does not display on the phone.

Set Up a Custom Background Image

Procedure

Step 1 Create two PNG files for each image (a full-size version and a thumbnail version). Ensure the PNG files comply with the format guidelines that are listed in Custom Background File Formats, on page 84.

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

Desktops/240x320x24

Note The file name and subdirectory parameters are case sensitive. Be sure to use the forward slash "/" when you specify the subdirectory path.

To upload the files, choose **Software Upgrades** > **Upload TFTP Server File** in Cisco Unified Communications Operating System Administration. For more information, see the documentation for your particular Cisco Unified Communications Manager release.

Note If the folder does not exist, the folder gets created and the files get uploaded to the folder.

Step 3 You must also copy the customized images and files to the other TFTP servers that the phone may contact to obtain these files.

Note We recommend that you store backup copies of custom image files in a different location. You can use these backup copies if the customized files are overwritten when you upgrade Cisco Unified Communications Manager.

Step 4 Use a text editor to edit the List.xml file. See Custom Background File Formats, on page 84 for the file location, file, formatting requirements, and a sample file.

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

Note When you upgrade Cisco Unified Communications Manager, a default List.xml file replaces your customized List.xml file. After you customize the List.xml file, make a copy of the file and store it in a different location. After upgrading Cisco Unified Communications Manager, replace the default List.xml file with your stored copy.

Step 6 To cache the new List.xml file, stop and start the TFTP service by using Cisco Unified Serviceability or disable and reenable the Enable Caching of Constant and Bin Files at Startup TFTP service parameter that is located in the Advanced Service Parameters area.

Custom Background File Formats

The List.xml file defines an XML object that contains a list of background images. The List.xml file is stored in the following subdirectory on the TFTP server:

Desktops/240x320x24

Tip If you are manually creating the directory structure and the List.xml file, you must ensure that the directories and files can be accessed by the user\CCMService, which is used by the TFTP service.

For more information, see the documentation for your particular Cisco Unified Communications Manager release.

The List.xml file can include up to 50 background images. The images are in the order that they appear in the Background Images menu on the phone. For each image, the List.xml file contains one element type, called ImageItem. The ImageItem element includes these two attributes:

- Image—Uniform resource identifier (URI) that specifies where the phone obtains the thumbnail image that appears on the Background Images menu on a phone.
- URL—URI that specifies where the phone obtains the full-size image.

The following example shows a List.xml file that defines two images. The required Image and URL attributes must be included for each image. The TFTP URI that is shown in the example is the only supported method for linking to full-size and thumbnail images. HTTP URL support is not provided.

List.xml Example

```
<CiscoIPPhoneImageList>
<ImageItem Image="TFTP:Desktops/240x320x24/TN-Fountain.png"
URL="TFTP:Desktops/800x480x24/Fountain.png"/>
<ImageItem Image="TFTP:Desktops/240x320x24/TN-FullMoon.png"
URL="TFTP:Desktops/800x480x24/FullMoon.png"/>
</CiscoIPPhoneImageList>
```

The phone firmware includes a default background image. The List.xml file does not define this image. The default image is always the first image that appears in the Background Images menu on the phone.

Each background image requires two PNG files:

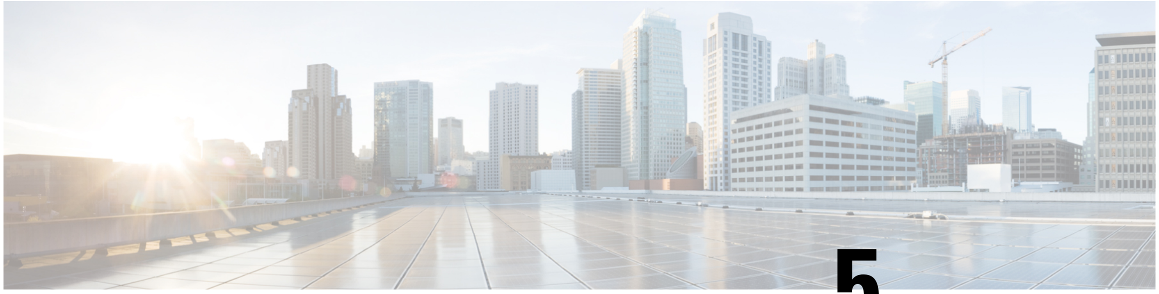
- Full size image—Version that appears on the on the phone.
- Thumbnail image—Version that displays on the Background Images screen from which users can select an image. Must be 25% of the size of the full-size image.

Tip Many graphics programs provide a feature that resizes a graphic. An easy way to create a thumbnail image is to first create and save the full-size image, then use the sizing feature in the graphics program to create a version of that image that is 25% of the original size. Save the thumbnail version by using a different name.

The PNG files for background images must meet the following requirements for proper display on the phone:

- Full size image—240 pixels (width) x 320 pixels (height).
- Thumbnail image—117 pixels (width) x 117 pixels (height).

Tip If you are using a graphics program that supports a posterize feature for grayscale, set the number of tonal levels per channel to 16, and the image posterizes to 16 shades of grayscale.



CHAPTER 5

Configuration on the Phone

Manually Set Up the Phone Network from the Settings Menu

When you are setting up the phone manually, you must set the following fields:

- IP address
- Subnet mask
- Default router
- DNS server 1
- TFTP server 1

After you set up the network configuration, you set up the Wi-Fi connection.

Procedure

Step 1 Access the **Settings** app.

Step 2 Select **Wi-Fi**.

Step 3 Select a profile.

Step 4 (Optional) Set a profile name.

a) Select **Profile name**

b) Enter the name of the profile

c) Press **More** ••• and select **Save**.

Step 5 Select **Network configuration** > **IPv4 Setup**.

Step 6 Select **DHCP** and press **Off**.

Step 7 Enter an IP address for the phone.

a) Select **IP address**.
b) Press the Navigation ring down and press **Select** to enter edit mode.
c) Enter the IP address.
d) Press **Save**.

Step 8 Enter a subnet mask.

a) Select **Subnet mask**.
b) Press the Navigation ring down and press **Select** to enter edit mode.
c) Enter the mask.
d) Press **Save**.

Step 9 Enter a default router.

a) Select **Subnet mask**.
b) Press the Navigation ring down and press **Select** to enter edit mode.
c) Enter the mask.
d) Press **Save**.

Step 10 Enter the primary DNS server.

a) Select **DNS server 1**.
b) Press the Navigation ring down and press **Select** to enter edit mode.
c) Enter the IP address of the DNS server.
d) Press **Save**.

Step 11 Enter the primary TFTP server

a) Select **TFTP server 1**.
b) Press the Navigation ring down and press **Select** to enter edit mode.
c) Enter the IP address of the TFTP server for your Cisco Unified Communications Manager.
d) Press **Save**.

Step 12 Press **Erase** at the Trust list prompt.

When you select **Erase**, the CTL and ITL files are removed from the phone. If you select **Continue**, the files remain but you may not be able to connect to the new Cisco Unified Communications Manager.

Related Topics

Reset the Network Settings, on page 133
Access the Settings App, on page 88

Access the Settings App

You use the **Settings** app to set up, manage, and customize your phone.

Procedure

Step 1 From the Line view screen, press the left arrow of the navigation cluster to view the Applications screen.

Step 2 From the Applications screen, press the left arrow of the navigation cluster to select **Settings** ⚙.

Add the Phone to the Wi-Fi Network

When you enter an IP address, scroll to the field, and press **Select**. The field changes from one field into input boxes. You use the keypad to enter the digits and the navigation ring to move between the fields.

After you configure the phone and save the changes, the phone connects to the Cisco Unified Communications Manager. After the connection is made, the phone downloads the configuration file and, if necessary, upgrades the firmware to a new firmware load.

Before you begin

You need the following information about the Wi-Fi network:

- SSID
- Security type (for example, WEP, EAP)
- PIN or passkey for the selected security type

Procedure

Step 1 Access the **Settings** app.

Step 2 Select **Wi-Fi**.

Step 3 Select a profile.

Step 4 (Optional) Set a profile name.

a) Select **Profile name**.

b) Use the keypad to enter a new name.

- The **Back** ⌫ softkey deletes the character to the left of the cursor.
- Use the Navigation ring to move from left to right in the field.

c) Press **More** ••• and select **Save**.

Step 5 Select **Network configuration** > **IPv4 setup**.

If your network does not support DHCP, perform these steps.

a) Required: Select **DHCP** and press **Off**.

b) Select **IP address** and enter the assigned address of the phone.

c) Select **Subnet mask** and enter the required subnet mask. For example, 255.255.255.0.

d) Select **Default router** and enter the IP address of the Default router.

e) Select **DNS server 1** and enter the IP address of the DNS server.

For all networks,

a) Select Alternate TFTP and set to **On**.

b) Select TFTP Server 1 and enter the TFTP IP address for the Cisco Unified Communications Manager.
c) Press **More** and select **Save**.
d) In the **Trust list** window, press **More** and select **Erase**.
e) Select **Back** and then select **Back** again.

Step 6 Select **WLAN configuration**.

Step 7 Select **SSID**.

a) Use the keypad to enter the SSID of the access point.
b) Press **More** and select **Save**.

Step 8 Select **Security mode**.

Step 9 Select the type of security that the access point requires.

Step 10 Set the required security fields using the following table:

Security Mode	Configured Field	Description
None	None	When the Security mode is set to None, no other fields are required.
WEP	WEP key	Enter the 40/104 or 64/128 ASCII or Hex WEP key.
PSK	Passphrase	Enter the 8-63 ASCII or 64 Hex Passphrase.
EAP-FAST PEAP-GTC PEAP-MSCHAPV2	User ID	Enter the userid.
	Password	Enter the password
EAP-TLS	User certificate	Select the type of certificate. You may need to give the certificate to your users. For more information, see Certificates, on page 31.

Step 11 Select **802.11 mode** and select the required mode.

The mode determines the frequency. If you set the mode to Auto, the phone can use either the 5 GHz or 2.4 GHz frequency, with 5 GHz as the preferred frequency.

Step 12 Select **On call power save** and press **Select** to change the setting.

This field should only be set to Disabled if required for troubleshooting.

Step 13 Press **More** and select **Save**.

Step 14 Press **Power/End Call** ☎.

Related Topics

Access the Settings App, on page 88

Connect the Phone to the Cisco Unified Communications Manager

Before you begin

- You need the IP address of the Cisco Unified Communications Manager TFTP server.
- The phone must be configured in the Cisco Unified Communications Manager
- The phone must be connected to the Wi-Fi network.

Procedure

Step 1 Access the **Settings** app.

Step 2 Select **Wi-Fi**.

Step 3 Select a profile.

Step 4 Select **Network configuration** > **IPv4**

Step 5 Select Alternate TFTP and set to **On**.

Step 6 Select TFTP Server 1 and enter the TFTP IP address for the Cisco Unified Communications Manager.

Step 7 Press **More** ••• and select **Set**.

Step 8 In the **Trust list** window, press **More** and select **Erase**.

When you select **Erase**, the CTL and ITL files are removed from the phone. If you select **Continue**, the files remain but you may not be able to connect to the new Cisco Unified Communications Manager.

Step 9 Exit to the home screen.

The phone connects to the Cisco Unified Communications Manager. After the connection is made, the phone downloads the configuration file and, if necessary, upgrades the firmware to a new firmware load.

Related Topics

Access the Settings App, on page 88

Cisco IP Phone Administration Page

Cisco phones that support Wi-Fi have special web pages that are different from the pages for other phones. You use these special web pages for phone security configuration when Simple Certificate Enrollment Protocol (SCEP) is not available. Use these pages to manually install security certificates on a phone, to download a security certificate, or to manually configure the phone date and time.

These web pages also show the same information that you see on other phone web pages, including device information, network setup, logs, and statistical information.

You can access the administration pages in these ways:

- wireless connection

- direct USB connection
- USB Ethernet dongle

Configure the Administration Page for Phone

The administration web page is enabled when the phone ships from the factory and the password is set to Cisco. But if a phone registers with Cisco Unified Communications Manager, the administration web page must be enabled and a new password configured.

Enable this web page and set the sign-in credentials before you use the web page for the first time after the phone has registered.

Once enabled, the administration web page is accessible at HTTPS port 8443 (**`https://x.x.x.x:8443`**, where x.x.x.x is a phone IP address).

Before you begin

Decide on a password before you enable the administration web page. The password can be any combination of letters or numbers, but it must be between 8 and 127 characters in length.

Your username is permanently set to admin.

Procedure

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

Step 2 Locate your phone.

Step 3 In the **Product Specific Configuration Layout**, set the Web Admin parameter to **Enable**.

Step 4 In the Admin Password field, enter a password.

Step 5 Select **Save** and click **OK**.

Step 6 Select **Apply Config** and click **OK**.

Step 7 Restart the phone.

Access the Phone Administration Web Page

When you want to access the administration web pages, you need to specify the administration port.

Procedure

Step 1 Obtain the IP address of the phone:

- In Cisco Unified Communications Manager Administration, select **Device** > **Phone**, and locate the phone. Phones that register with Cisco Unified Communications Manager display the IP address on the **Find and List Phones** window and at the top of the **Phone Configuration** window.
- On the phone, access the **Settings** app, choose **Phone Information** > **Network** > **IPv4**, and then scroll to the IP address field.

Step 2 Open a web browser and enter the following URL, where *IP_address* is the IP address of the Cisco IP Phone:

```
https://<IP_address>:8443
```

Step 3 Enter the password in the Password field.

Step 4 Click **Submit**.

Related Topics

Access the Settings App, on page 88

Set Up the Phone with the Administration Web Page

You can set the phone parameters from the Administration web page if you need to set up the phone remotely. When you set up the phone this way, you set up the first WLAN profile for the phone.

Procedure

Step 1 From the phone administration web page, select **WLAN**.

Step 2 Click **Profile 1**.

Step 3 Set the fields as described in the following table.

Field Name	Description
Source	Read-only field
Status	Use to enable or disable the profile.
Profile	Enter the name of the profile.
User modifiable	Set the field to enable or disable the user from changing their WLAN profile.
WLAN configuration	
SSID	Enter the SSID of the access point.
Security mode	Select a security mode.
WEP key	When the security type is set to WEP, the screen changes to display the **WEP key** field. enter a 40/104 or 64/128 ASCII or Hex WEP key.
Passphrase	When the security type is set to PSK, the screen changes to display the **Passphrase** field. Enter an 8-63 ASCII or 64Hex passphrase.
User ID	When the security type is EAP-Fast, PEAP-GTC, or PEAP-MSCHAPV2, the screen changes to display the **User ID** field. Enter the id of the user.

Field Name	Description
Password	When the security type is EAP-Fast, PEAP-GTC, or PEAP-MSCHAPV2, the screen changes to display the **Password** field. Enter a password.
User certificate	Select the type of certificate.
802.11 mode	Select the mode required.
On call power save	Select the type of power save mode that the phone uses to save power.
Network configuration	
Domain name	Enter the domain name.
IPv4 setup	
DHCP	Set your DHCP method. If DHCP is off, you have more fields to set up.
IP address	When DHCP is off, assign a static IP address
Subnet mask	When DHCP is off, enter the subnet mask.
Default router	When DHCP is off, enter the IP address of the router.
DNS server 1 DNS server 2 DNS server 3	When DHCP is off, enter the IP address of at least one DNS server.
Alternate TFTP	Set this field to indicate if you use a different TFTP server from the one associated with your Cisco Unified Communications Manager.
TFTP server 1 TFTP server 2	Enter the IP address of the Cisco Unified Communications Manager TFTP server (primary and, if available, secondary).

Step 4 Click **Save**.

Configure Backup Settings from the Phone Administration Web Page

You can use the phone administration web page to backup and restore the phone configuration.

Procedure

Step 1 From the phone administration web page, select **Backup settings**.

Step 2 Perform one of the following options:

- Import a backup file. Browse to the file on your computer, enter the encryption key, and click **Import**.
- Export a backup file. Enter an encryption key and click **Export**. Remember that you will need this key to import the file.

Manually Set the Phone Date and Time

With certificate-based authentication, the phone must display the correct date and time. An authentication server checks the phone date and time against the certificate expiry date. If the phone and the server dates and times don't match, the phone stops working.

Use this procedure to manually set the date and time on the phone if the phone is not receiving the correct information from your network.

Procedure

Step 1 From the phone administration web page, scroll to **Date and time**.

Step 2 Perform one of the following options:

- Click **Set phone to local date and time** to synch the phone to a local server.
- In the **Specify date and time fields**, select the month, day, year, hour, minute, and second using the menus and click **Set phone to specific date and time**.

Local Contacts Management from the Phone Administration Page

Through the phone administration web page, you can:

- Import a comma separated values (CSV) file of contacts into the user's phone.
- Export a user's local contacts list as a CSV file.
- Delete all the local contacts from a user's phone.

The import and export functions can be useful during initial phone setup. You could set up a list of commonly-used phone numbers for your organization on one phone. Then you could export that list and import it to other phones.

If you allow your users to access the phone administration page, make sure that you give them the local contacts import and export instructions.

Recommended Approach for Initial Local Contacts Lists

If you want to create a list to import to multiple phones, this approach is recommended:

1. Create a single entry in the local contacts list of a phone.
2. Export the list from the phone.

3. Edit the list to add the entries.

   You can use a text editor to edit the list.

   If you use other tools (for example, document or spreadsheet programs), you need to save the list in one of these formats:

   - CSV UTF-8
   - Standard CSV

4. Import the list into the phone.
5. Verify that the list is displayed correctly before you import it on other phones.

Import a User's Local Contacts

You can import a CSV file into a user's phone. You can create this CSV file using a text editor or create the list on one phone and export it (see Export a User's Local Contacts, on page 97).

You can add up to 200 Local contacts. However, if a Local contacts list already exists on the phone, the number of entries in the CSV file and in the phone can't exceed 200, or the import fails.

Only 49 of the entries can be marked as Favorites, because the first entry in the Favorites list is reserved for voicemail. If a Favorites list already exists on the phone, the number of entries in the CSV file that are marked as favorites and the number in the phone can't exceed 49, or the import fails.

The import does not check to see if the entries already exist in the phone, so duplicated entries are possible. Duplicated entries must be manually deleted.

Before you begin

Create a CSV file in the following format.

Sample CSV file

```
First name, Last name, Nickname, Company, Work number, Home number, Mobile number, Email
address, Work primary, Home primary, Mobile primary, Work favorite, Home favorite, Mobile
favorite
Michael,G,,Sample Company,1000,12345678,,test@test.com,true,false,false,2,3,
```

Where:

Field Name	Description	From the Sample
First name	First name as a string	Michael
Last name	Last name as a string, or leave empty	G
Nickname	Short name as a string, or leave empty	(empty)
Company	The company name as a string, or leave empty. **Note** The string cannot contain a comma.	Sample Company

Field Name	Description	From the Sample
Work number	The exact number to be dialed from the phone.	1000
Home number	The exact number to be dialed from the phone.	12345678
Mobile number	The exact number to be dialed from the phone.	(empty)
Email address	An email address, or leave empty	test@test.com
Work primary Home primary Mobile primary	Values—true, false Configure only one of these values to be true, and the other two are configured as false.	Work primary—true Home primary—false Mobile primary—false
Work favorite Home favorite Mobile favorite	Configure the Favorite slot number for any numbers to be added to Favorites. For example, enter 2 in Work favorite to map the Work number to Favorite slot 2. **Note** Favorite slot 1 is reserved for voicemail.	Work favorite—2 Home favorite—3 Mobile favorite—(empty)

Procedure

Step 1 From the phone administration web page, select **Local contacts**.

Step 2 Under **Import local contacts**, click **Browse**.

Step 3 Navigate to the CSV file, click on it, and click **OK**.

Step 4 Click **Upload**.

Step 5 Check on the phone to ensure that the list is displayed correctly.

Export a User's Local Contacts

You can export a phone's local contacts list as a CSV file.

Procedure

Step 1 From the phone administration web page, select **Local contacts**.

Step 2 Under **Export local contacts**, click **Export**.

Step 3 Save the file on your computer.

Delete a User's Local Contacts

You can delete the complete local contacts list from a phone. For example, you might do this before you assign the phone to another user.

Procedure

Step 1 From the phone administration web page, select **Local contacts**.

Step 2 Under **Delete all local contacts**, click **Delete**.

Step 3 In the pop-up window, confirm the deletion.

Step 4 Check that the local contacts list on the phone is empty.

Wireless LAN Security

Cisco phones that support Wi-Fi have more security requirements and require extra configuration. These extra steps include installing certificates and setting up security on the phones and on the Cisco Unified Communications Manager.

For additional information, see *Security Guide for Cisco Unified Communications Manager*.

Install a User Certificate from the Phone Administration Web Page

You can manually install a user certificate on the phone if Simple Certificate Enrollment Protocol (SCEP) is not available.

The preinstalled Manufacturing Installed Certificate (MIC) can be used as the User Certificate for EAP-TLS.

After the User Certificate installs, you need to add it to the RADIUS server trust list.

Before you begin

Before you can install a User Certificate for a phone, you must have:

- A User Certificate saved on your PC. The certificate must be in PKCS #12 format.
- The certificate's extract password.

Procedure

Step 1 From the phone administration web page, select **Certificates**.

Step 2 Locate the **User installed** field and click **Install**.

Step 3 Browse to the certificate on your PC.

Step 4 In the **Extract password** field, enter the certificate extract password.

Step 5 Click **Upload**.

Step 6 Restart the phone after the upload is complete.

Install an Authentication Server Certificate from the Phone Administration Web Page

You can manually install an Authentication Server certificate on the phone if Simple Certificate Enrollment Protocol (SCEP) is not available.

The root CA certificate that issued the RADIUS server certificate must be installed for EAP-TLS.

Before you begin

Before you can install a certificate on a phone, you must have an Authentication Server Certificate saved on your PC. The certificate must be encoded in PEM (Base-64) or DER.

Procedure

Step 1 From the phone administration web page, select **Certificates**.

Step 2 Locate the **Authentication server CA (Admin webpage)** field and click **Install**.

Step 3 Browse to the certificate on your PC.

Step 4 Click **Upload**.

Step 5 Restart the phone after the upload is complete.

If you are installing more than one certificate, install all of the certificates before restarting the phone.

Manually Remove a Security Certificate from the Phone Administration Web Page

You can manually remove a security certificate from a phone if Simple Certificate Enrollment Protocol (SCEP) is not available.

Procedure

Step 1 From the phone administration web page, select **Certificates**.

Step 2 Locate the certificate on the **Certificates** page.

Step 3 Click **Delete**.

Step 4 Restart the phone after the deletion process completes.

SCEP Setup

Simple Certificate Enrollment Protocol (SCEP) is the standard for automatically provisioning and renewing certificates. It avoids manual installation of certificates on your phones.

Configure the SCEP Product Specific Configuration Parameters

You must configure the following SCEP parameters on your phone web page

- RA IP address
- SHA-1 or SHA-256 fingerprint of the root CA certificate for the SCEP server

The Cisco IOS Registration Authority (RA) serves as a proxy to the SCEP server. The SCEP client on the phone use the parameters that are downloaded from Cisco Unified Communication Manager. After you configure the parameters, the phone sends a `SCEP getcs` request to the RA and the root CA certificate is validated using the defined fingerprint.

Procedure

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

Step 2 Locate the phone.

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

Step 4 Check the **WLAN SCEP Server** check box to activate the SCEP parameter.

Step 5 Check the **WLAN Root CA Fingerprint (SHA256 or SHA1)** check box to activate the SCEP QED parameter.

Simple Certificate Enrollment Protocol Server Support

If you are using a Simple Certificate Enrollment Protocol (SCEP) server, the server can automatically maintain your user and server certificates. On the SCEP server, configure the SCEP Registration Agent (RA) to:

- Act as a PKI trust point
- Act as a PKI RA
- Perform device authentication using a RADIUS server

For more information, see your SCEP server documentation.

Set Up a Phone with the USB Dongle and the Desktop Charger

A USB to Ethernet adapter (dongle) can be inserted into the desktop charger to connect to an Ethernet network for automatic Wi-Fi profile provisioning and certificate enrollment purposes only. Voice calls over the Ethernet network are not supported.

Note The USB Dongle is not intended to be connected to the desktop charger for day-to-day use. It is intended to be only used for initial provisioning purposes.

The native VLAN of the switch port to be used for provisioning must have connectivity to the Cisco Unified Communications Manager and must offer DHCP option 150 pointing it to the Cisco Unified Communications Manager.

The supported USB to Ethernet adapters are:

- Apple USB 2.0 Ethernet Adapter
- Belkin B2B048 USB 3.0 Gigabit Ethernet Adapter
- D-Link DUB-E100 USB 2.0 Fast Ethernet Adapter
- Linksys USB300M USB 2.0 Ethernet Adapter
- Linksys USB3GIG USB 3.0 Gigabit Ethernet Adapter

Before you begin

You need a USB to Ethernet adapter (dongle).

The desktop charger must be connected to the power source using the power adapter.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, check that the WLAN Profile you created is associated to either the correct CUCM device pool (**System** > **Device Pool**), or associated with the wireless phone (**Device** > **Phone**).

Step 2 Connect one end of the dongle into the desktop charger and the other end to an RJ-45 cable connected to the network switch.

Step 3 Put the phone into the desktop charger and wait while the profile downloads.

Step 4 Check that the phone registers to the Cisco Unified Communications Manager.

Step 5 Remove the phone from the desktop charger.

Step 6 Disconnect the dongle from the desktop charger.

CHAPTER 6

Accessories

Supported Accessories

You can use a number of accessories with your phone.

- Headsets:
  - Standard headsets that use a 3.5 mm jack
  - Bluetooth headsets
- Cisco Wireless IP Phone 8821 Desktop Charger: charges the Cisco Wireless IP Phone 8821 only
- Cisco Wireless IP Phone 8821-EX Desktop Charger: charges the Cisco Wireless IP Phone 8821-EX only
- Cisco Wireless IP Phone 8821 Multi Charger: charges the Cisco Wireless IP Phone 8821 only
- Cisco Wireless IP Phone 8821-EX Multi Charger: charges the Cisco Wireless IP Phone 8821-EX only

Note The Cisco Wireless IP Phone 8821-EX has not been tested or certified with any accessories for use in Potentially Explosive Atmosphere.

The phones can only connect to Bluetooth headsets and speakers. They do not support any other type of Bluetooth device.

For more information on accessories, see the *Cisco Wireless IP Phone 882x Series Accessory Guide*, located here: http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-user-guide-list.html.

Headsets

You can use wired and Bluetooth headsets with your phone. For information about the supported headsets, see the *Cisco Wireless IP Phone 882x Series Accessory Guide*.

Although we perform some internal testing of third-party wired and Bluetooth wireless headsets for use with the Cisco Wireless IP Phone 8821 and 8821-EX, we do not certify or support products from headset or handset vendors. Because of the inherent environmental and hardware inconsistencies in the locations where phones are deployed, there is not a single “best” solution that is optimal for all environments. We recommend that customers test the headsets that work best in their environment before deploying a large number of units in their network.

Note The Cisco Wireless IP Phone 8821-EX has not been tested for wired and Bluetooth headsets in hazardous locations.

We recommend 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.

The primary reason that a particular headset would be inappropriate for the phone is the potential for an audible hum. This hum can be heard by either the remote party or by both the remote party and you, the phone user. Some potential humming or buzzing sounds can be caused by a range of outside sources, for example, electric lights, 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 phone users.

Standard Headsets

You can use a wired headset with your phone. The headset requires a 3.5 mm, 3-band, 4-connector plug.

If you plug a headset into the phone during an active call, the audio path automatically changes to the headset.

Bluetooth Headsets

You can use a Bluetooth headset with your phone. When you use a Bluetooth wireless headsets, the headset usually increases battery power consumption on your phone and may 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.

Desktop Chargers

You can use the Cisco Wireless IP Phone 8821 Desktop Charger to charge your Cisco Wireless IP Phone 8821 and spare phone battery. The charger works on AC power or from a charged spare phone battery. It can be secured with a standard laptop cable lock. This charger has a label on the back to show the maximum voltage (4.35 V).

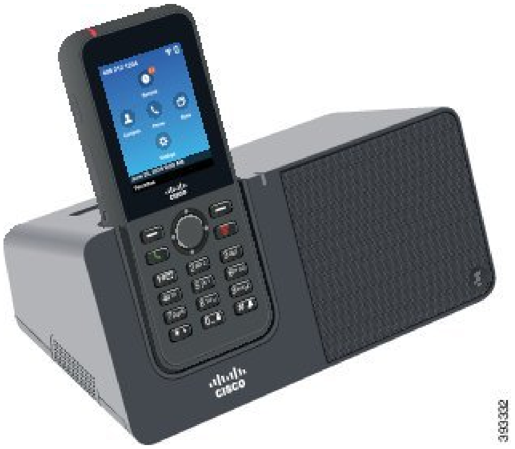
You can use the Cisco Wireless IP Phone 8821-EX Desktop Charger to charge your Cisco Wireless IP Phone 8821-EX and spare phone battery. The charger works on AC power or from a charged spare phone battery.

It can be secured with a standard laptop cable lock. The charger looks the same as the Cisco Wireless IP Phone 8821 Desktop Charger except that it shows the graphic of the Cisco Wireless IP Phone 8821-EX and doesn't have the voltage label.

Caution The Cisco Wireless IP Phone 8821 Desktop Charger can only charge the Cisco Wireless IP Phone 8821 and a spare battery for that phone. You can't charge the Cisco Wireless IP Phone 8821-EX or its spare batteries in the Cisco Wireless IP Phone 8821 Desktop Charger.

The following figure shows the Cisco Wireless IP Phone 8821 Desktop Charger with a Cisco Wireless IP Phone 8821.

Figure 4: Cisco Wireless IP Phone 8821 and Cisco Wireless IP Phone 8821 Desktop Charger



Caution Do not use the desktop charger in a hazardous environment.

The desktop charger also allows you to use your phone in handsfree mode.

In this document, the term *desktop charger* refers to both chargers.

Set Up the Desktop Charger

You should place the desktop charger on a stable work surface.

Before you begin

You need the cable that is provided with the charger. This cable has a plug on one end and a USB connector on the other end.

You need the power adapter that comes with the phone.

Procedure

Step 1 Plug the plug end of the cable into the desktop charger.

Step 2 Plug the USB end of the cable into the power adapter and plug the power adapter into the electrical outlet.

Charge Your Phone with the Desktop Charger

You can tell when your phone is charging in the charger when the phone LED lights red and a message or icon displays on the phone screen. When the battery is fully charged, the LED turns green. Your phone can take up to 3 hours to recharge.

If your phone has a protective case, you don't need to remove the case before you charge the phone in the desktop charger. You adapt the charger to fit the phone.

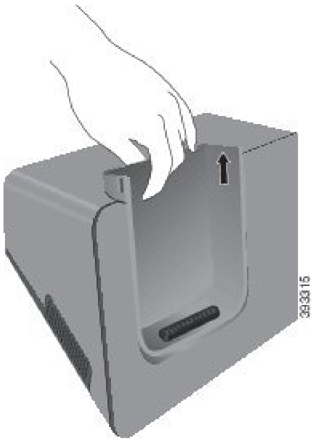
When you put the phone into the charger, make sure that you align the charging pins on the bottom of the phone with the connector in the charger. When the phone is correctly placed in the charger, it is held in place with magnets. If the LED does not light, then the alignment is not correct.

Caution Do not charge the phone in a hazardous environment.

Do not charge the phone if it is wet.

Procedure

Step 1 (Optional) Adapt the charger for a phone in a case: Turn the charger so that the back is facing you, put three fingers about 3/4 of the way into the cup, press in, and lift. The cup should slide out.



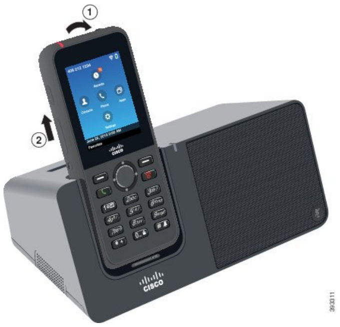
Note You might need to use two hands to remove the cup the first time.

Step 2 Place your phone in the charging slot with the screen facing towards you. If your phone is in a case, press the phone into the charging slot to ensure that the phone connects with the contacts.

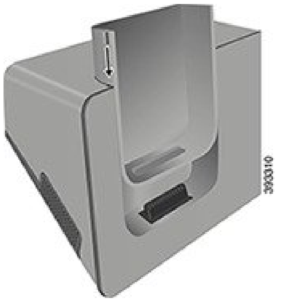
Make sure that the LED on the phone lights red. If the LED does not light up, remove the phone and reinsert it into the charger.

If your phone is in a case, the phone and case will tilt out because of the case.

Step 3 When you remove the phone from the charger, tilt the phone forward and lift it up to disconnect the connecter from the magnets.



Step 4 (Optional) Slide the charging cup into the charger. Make sure that the cup is flush with the front and top of the charger.



Charge Your Spare Battery with the Desktop Charger

You can charge a spare battery in the desktop charger. The battery can take up to 3 hours to charge.

⚠ **Caution** Do not charge the battery in a hazardous environment.

When the battery is charging, the spare battery LED on the charger lights red. When the battery is charged, the spare battery LED on the charger lights green.

Procedure

Step 1 Hold the battery so that the Cisco label faces you, and the arrows on the battery point down.

Step 2 Place the spare battery in the slot behind the phone cradle and press down firmly.

Multichargers

You can charge up to six Cisco Wireless IP Phone 8821 and six spare batteries at the same time with the Cisco Wireless IP Phone 8821 Multi Charger. If your phone is in a protective case, you can charge it without removing the case. This charger has a label on the back to show the maximum voltage (4.35 V).

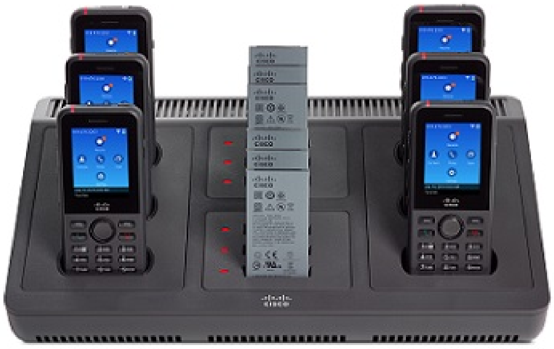
You can charge up to six Cisco Wireless IP Phone 8821-EX and six spare batteries at the same time with the Cisco Wireless IP Phone 8821-EX Multi Charger. If your phone is in a protective case, you can charge it without removing the case. The charger looks the same as the Cisco Wireless IP Phone 8821 Multi Charger except that it shows the graphic of the Cisco Wireless IP Phone 8821-EX and doesn't have the voltage label.

⚠

Caution The Cisco Wireless IP Phone 8821 Multi Charger can only charge the Cisco Wireless IP Phone 8821 and a spare battery for that phone. You can't charge the Cisco Wireless IP Phone 8821-EX or its spare batteries in the Cisco Wireless IP Phone 8821 Multi Charger.

The following figure shows the multicharger. The phones are placed in the charging cups on the left and right, and the spare batteries are placed in the center.

Figure 5: Cisco Wireless IP Phone 8821 and Cisco Wireless IP Phone 8821 Multi Charger



⚠

Caution Do not use the multicharger in a hazardous environment.

The multicharger can be placed on a work surface or mounted on a wall with the wall mount kit.

In this document, the term *multicharger* refers to both chargers.

Set Up the Multicharger

The power jack is on the right side of the multicharger.

Procedure

Step 1 Plug the jack end of the power cord into the multicharger.

Step 2 Plug the other end of the power cord into the power adapter.

Step 3 Plug the power adapter into the electrical outlet.

Step 4 Place the multicharger on a stable work surface.

Install the Multicharger Wall Mount Kit

The wall mount kit comes with the following components:

- bracket
- package with 5 screws and 5 self-tapping wall anchors

Before you begin

You need the following tools:

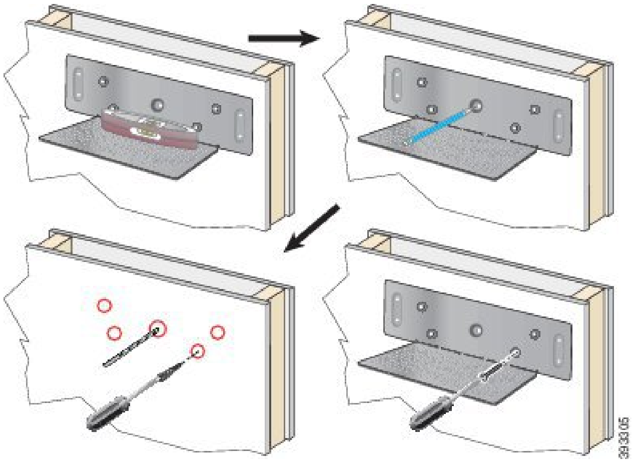
- Drill and a 0.25 inch drill bit
- Pencil
- Level
- Philips #1 and #2 screwdrivers

You need the power cable and power adapter.

Procedure

Step 1 Determine the location for the bracket. The bottom right corner of the bracket must be less than 50 inches (127 cm) from an electrical outlet.

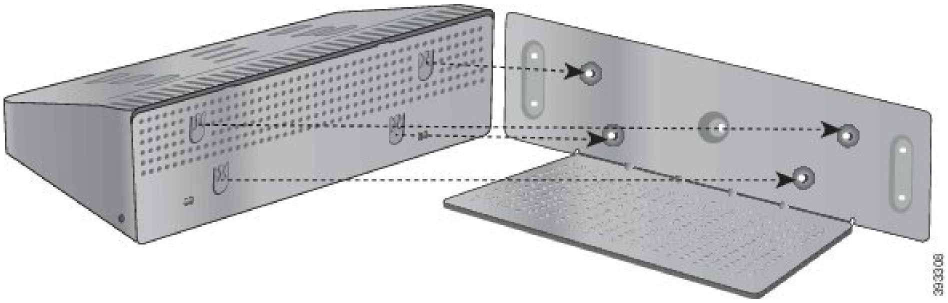
Step 2 Mount the wall bracket.



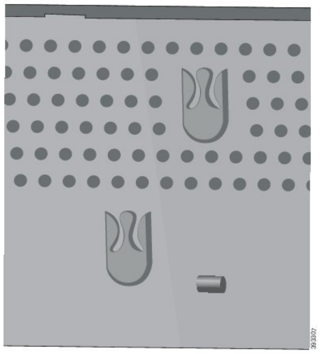
a) Hold the bracket on the wall, as shown in the diagram.
b) Use the level to ensure that the bracket is level and use a pencil to mark the screw holes.
c) Install the anchors, using the drill and drill bit.
d) Screw the bracket to the wall.

Step 3 Locate the post holders in the multicharger.

Step 4 Hold the multicharger so that the post holders are in front of the posts on the bracket, press the multicharger towards the wall, and then push the multicharger down so that the posts seat into the holder.



Here is a close-up of the post holder.



Step 5 Plug the jack end of the power cord into the multicharger.

Step 6 Plug the other end of the power cord into the power adapter.

Step 7 Plug the power adapter into the electrical outlet.

Charge Your Phone with the Multicharger

You can tell when your phone is charging in the multicharger when the phone LED lights red. When the battery is fully charged, the LED turns green. Your phone can take up to 3 hours to recharge.

If your phone has a protective case, you don't need to remove the case before you charge the phone in the multicharger. You adapt the multicharger to fit the phone.

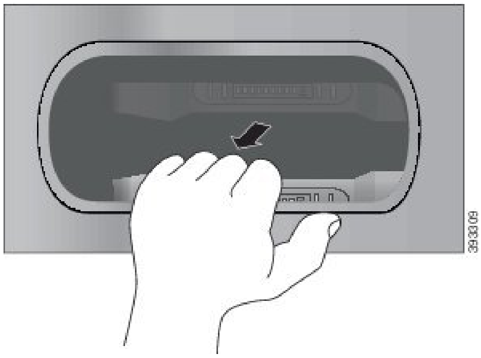
When you put the phone into the multicharger, make sure that you align the charging pins on the bottom of the phone with the connector in the multicharger. If the LED does not light, then the alignment is not correct.

⚠ **Caution** Do not charge the phone in a hazardous environment.

Do not charge the phone if it is wet.

Procedure

Step 1 (Optional) Adapt the charger for a phone in a case: Reach into the cup with three fingers, locate the slots on the inside of the cup, and use the slots to pull the cup out.



Step 2 Place your phone in the empty charging slot. If your phone is in a case, press the phone into the charging slot to ensure that the phone connects with the contacts.

Make sure that the LED on the phone lights red. If the LED does not light up, remove the phone and reinsert it into the multicharger.

Step 3 (Optional) Slide the charging cup into the multicharger and press the cup into place so that the cup is flush with the top of the multicharger.

Charge Your Spare Battery with the Multicharger

You can charge a spare battery in the multicharger. The battery can take up to 3 hours to charge.

⚠ **Caution** Do not charge the battery in a hazardous environment.

When the battery is charging, the Battery LED beside the battery lights red. When the battery is charged, the Battery LED lights green.

Procedure

Place the battery in an empty spare battery slot, aligning the battery contacts with the charger connecter.

If the Battery LED does not light red, remove the battery and reinsert it into the battery slot.

Secure the Charger with a Cable Lock

You can secure your desktop charger or multicharger with a laptop cable lock that is up to 20 mm wide.

Procedure

Step 1 Take the looped end of the cable lock and wrap it around the object to which you want to secure your phone.
Step 2 Pass the lock through the looped end of the cable.
Step 3 Unlock the cable lock.
Step 4 Press and hold the locking button to align the locking teeth.
Step 5 Insert the cable lock into the lock slot of your charger and release the locking button.
Step 6 Lock the cable lock.

CHAPTER 7

Phone Statistics

Statistics Available on the Phone

You can see statistics and information about the phone from the **Settings** menu on the phone.

These menus help you troubleshoot problems when you are in the same location as your user.

View Phone Information

When you troubleshoot phone problems, you often need information from the phone.

Procedure

Step 1 Access the **Settings** app.

Step 2 Select **Phone information**.

Related Topics

Access the Settings App, on page 88

Access Device Information

The Device information menu and submenus provide information related to the connections between the phone and the call control system.

Procedure

Step 1 Access the **Settings** app.

Step 2 Select **Phone information** > **Device information**.

Step 3 Select one of the following entries.

- **Call manager**—displays information about the call control system.

- **Network**—displays information about the IPv4 network.
- **WLAN**—displays information about the Wi-Fi connection.
- **HTTP**—displays information about configured URLs.
- **Locale**—displays information about the language locale.
- **Security**—displays information about the security settings.
- **QoS**—displays information related to the Quality of Service.
- **UI**—displays information related to the user interface.
- **Battery**—displays information related to the battery.

Related Topics

Access the Settings App, on page 88

Device Information

The following tables describe the submenus and fields in the **Device Information** menu.

Table 7: Menu: Cisco Unified CM

Field	Description
Cisco Unified CM 1	Primary call manager server that the phone uses. Displays the IP address and status.
Cisco Unified CM 2	Secondary call manager server that the phones uses. Displays the IP address and status, or is blank if not in use.
Cisco Unified CM 3	Displays the IP address and status of an additional call manager server, or is blank if not in use.
Cisco Unified CM 4	Displays the IP address and status of an additional call manager server, or is blank if not in use.
Cisco Unified CM 5	Displays the IP address and status of an additional call manager server, or is blank if not in use.

Any of these call manager fields can also show the IP address of an SRST router that is capable of providing limited call control system functionality.

Each available server displays the server IP address and one of the following states:

Active

Call control system from which the phone is currently receiving call-processing services.

Standby

Call control system to which the phone switches if the current server becomes unavailable.

Blank

No current connection to this Call control system.

Table 8: Menu: Network > IPv4

Field	Description
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.
DHCP server	IP address of the DHCP server from which the phone obtains its IP address.
IP address	IP address of the phone.
Subnet mask	Subnet mask used by the phone.
Default router	IP address for the default gateway used by the phone.
DNS server 1	Primary DNS server used by the phone.
DNS server 2	First backup DNS server used by the phone.
DNS server 3	Second backup DNS server used by the phone.
Alternate TFTP	Address of the TFTP server (other than the one assigned by DHCP).
TFTP server1	Primary TFTP server used by the phone.
TFTP server 2	Secondary TFTP server used by the phone.
Load server	Host name or IP address for the alternate server that the phone uses for firmware upgrades.
BOOTP server	
CDP	Cisco Discovery Protocol (CDP) usage.
GARP	Gratuitous ARP used for MAC address discovery.

Table 9: Menu: WLAN

Field Name	Description
Profile name	Name of the network profile that the phone is currently using.
SSID	Service Set ID (SSID) that the phone is currently using.
Security mode	Authentication method that the phone is currently using in the wireless network.
802.11 mode	Wireless signal mode that the phone is currently using.
On call power save	Type of power save mode that the phone uses to save battery power: PS-Poll or U-APSD.

Field Name	Description
Scan mode	Type of AP scanning.
WLAN SCEP server	URL or host name of the Simple Certificate Enrollment Protocol (SCEP)server
WLAN Root CA fingerprint	SHA256 or SHA1 fingerprint of the Root CA for WLAN authentication.

Table 10: Menu: HTTP

Field Name	Description
Authentication URL	URL that the phone uses to validate requests made to the phone web server.
Directories URL	URL of the server from which the phone obtains directory information.
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 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.
Information URL	URL of the help text that appears on the phone.
Messages URL	URL of the server from which the phone obtains message services.
IP phone proxy address	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.
Services URL	URL of the server from which the phone obtains phone services.
Secured authentication URL	Secure URL that the phone uses to validate requests made to the phone web server.
Secured directory URL	Secure URL of the server from which the phone obtains directory information.
Secured idle URL	Secure 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.
Secured information URL	Secure URL of the help text that appears on the phone.
Secured messages URL	Secure URL of the server from which the phone obtains message services.
Secured services URL	Secure URL of the server from which the phone obtains phone services.

Table 11: Menu: Locale

Field	Description
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.

Table 12: Menu: Security

Field	Description
Web access	Indicated web access capability for the phone. **Disabled** No self care portal access. **ReadOnly** Can view information only. **Enabled: HTTP and HTTPS** Can use the configuration pages
Web admin	Indicates if the web admin page is enabled.
Security mode	Security mode assigned to the phone

Table 13: Menu: QoS

Field Name	Description
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.

Table 14: Menu: UI

Field Name	Description
BLF for call lists	Indicates whether the Busy Lamp Field (BLF) is enabled for call lists.

Field Name	Description
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.

Table 15: Menu: Battery

Field Name	Description
Battery health	Indicates the overall health of the battery.
Battery temperature	Indicates the current temperature of the battery. If the battery runs excessively hot, the battery may fail soon.
Battery level	Indicates the current charge level of the battery.

Access Model Information

The Model information menu provides information related to the phone model.

Procedure

Step 1 Access the **Settings** app.

Step 2 Select **Phone information** > **Model information**.

Related Topics

Access the Settings App, on page 88

Model Information

The following table describes the fields and contents in the **Phone information** > **Model information** screen.

Table 16: Model Information Fields

Field Name	Description
Model number	Set to CP-8821 or CP-8821-EX
MAC address	MAC address of the phone
App load ID	Firmware version running on the phone
Serial number	Phone serial number
USB vendor ID	Set to Cisco
USB product ID	Set to 8821 or 8821-EX

Field Name	Description
RNDIS device address	Remote Network Device Interface Specification (RNDIS) address of the USB
RNDIS host address	RNDIS for the USB

Access Firmware Version

The Firmware version menu provides information related to the firmware running on the phone.

Procedure

Step 1 Access the **Settings** app.

Step 2 Select **Phone information** > **Firmware version**.

Related Topics

Access the Settings App, on page 88

Firmware Version Information

The following table describes the fields and contents in the **Phone information** > **Firmware version** screen.

Table 17: Firmware Version Fields

Field Name	Description
Active load	Firmware load that is active
Last upgrade	Upgrade status: date and time for successful update; otherwise messages about upgrade failure
Boot load ID	Identification of the boot loader version
WLAN driver ID	Identification of the WLAN driver
WLAN firmware ID	Identification of the WLAN firmware load

Phone Statistics in the Admin Settings Menu

You can access some statistics about the phone from the **Admin settings** menu. These are the same statistics that are displayed if you access the phone from the administration web page.

Neighbor List Menu

The **Neighbor list** from the **Admin settings** menu shows the available access points.

Access the Status Menu

The Status menu on the phone gives you important information about the phone.

Procedure

Step 1 Access the **Settings** app.

Step 2 Select **Admin settings** > **Status**.

Related Topics

Access the Settings App, on page 88

Status Messages

The **Status messages** screen provides a list of status messages. Each message has a date and time stamp. You can use these messages to troubleshoot problems.

WLAN Statistics

Table 18: WLAN Statistics Fields

Field	Description
tx bytes	Number of bytes transmitted
rx bytes	Number of bytes received
tx packets	Number of packet transmitted
rx packets	Number of packet received
tx packets dropped	Number of packets transmitted that were dropped
rx packets dropped	Number of packets received that were dropped
tx packets errors	Number of transmitted packet errors
rx packets errors	Number of transmitted packet errors
tx frames	Number of frames transmitted
tx multicast frames	Number of multicast frames transmitted
tx retry	Number of transmission retries
tx multi retry	Number of muilticast transmission retries
tx failure	Number of transmission failures
rts success	Number of request to send (rts) successes
rts failure	Number of rts failures
ack failure	
rx duplicate frames	Number of duplicate frames received
rx fragmented packets	Number of fragmented packets received

Field	Description
Roaming count	

Call Statistics

Field	Description
Receiver codec	Type of audio encoding received by the phone: G.729, G.711 u-law, G.711 A-law
Sender codec	Type of audio encoding sent by the phone: G.729, G.711 u-law, G.711 A-law
Receiver size	
Sender size	
Rcvr packets	Number of packets received by the phone
Sender packets	
Transmitter DSCP	
Receiver DSCP	
Transmitter WMM UP	Wireless Multi Media (WMM) Up transmitter
Receiver WMM UP	Wireless Multi Media (WMM) Up receiver
Avg jitter	Estimated average RTP packet jitter (dynamic delay that a packet encounters when going through the network).
Max jitter	Maximum jitter observed since the receiving voice stream was opened.
Receiver discarded	
Rcvr lost packets	
Cumulative conceal ratio	Total number of concealment frames divided by total number of speech frames received from start of the voice stream.
Interval conceal ratio	Ratio of concealment frames to speech frames in preceding 3-second interval of active speech. If using voice activity detection (VAD), a longer interval might be required to accumulate 3 seconds of active speech.
Max conceal ratio	Highest interval concealment ratio from start of the voice stream.

Field	Description
Severely conceal seconds	Number of seconds that have more than 5 percent concealment events (lost frames) from the start of the voice stream.
Latency	

Trace Settings

The **Trace settings** menu gives you information for troubleshooting parameters.

Field	Description
Remote syslog	Support of remote system logging
Log profile	Type of logging
Additional debugs	Not currently supported

Statistics Available from the Phone Web Pages

You can use the phone web pages to see statistics and other phone information from the web. These pages display the same information that you can see if you access the statistics on the phone.

These pages can help you troubleshoot problems, no matter where your user is located.

Access Web Page for Phone

To access the web page for a phone, follow these steps:

Note If you cannot access the web page, it may be disabled by default.

Procedure

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

a) Search for the phone in Cisco Unified Communications Manager Administration by choosing **Device** > **Phone**. Phones that register with Cisco Unified Communications Manager display the IP address on the **Find and List Phones** window and at the top of the **Phone Configuration** window.

b) On the Cisco IP Phone, access the **Settings** app, select **Phone information** > **Device information** > **Network** > **IPv4**, and then scroll to the IP Address field.

Step 2 Open a web browser and enter the following URL, where *IP_address* is the IP address of the Cisco IP Phone:

`http://`*IP_address*

Related Topics

Access the Settings App, on page 88

Device Information Web Page

The **Device Information** page is the first page you see when you access the Phone web pages. Use the left pane to navigate to the other pages.

Field	Description
Active network interface	Active network type
MAC address	Media Access Control (MAC) address of the phone
Wireless MAC address	Wireless 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.
Phone DN	Directory number assigned to the phone
App load ID	Firmware version running on the phone
Boot load ID	Version of the boot firmware
Version	Firmware version running on the phone
Hardware revision	Version of the phone hardware
Serial number	Serial number of the phone
Model number	Model name of the phone
Message waiting	State of the message waiting indicator
UDI	Information about the phone (type, model name, model ID, hardware version, and serial number)
Time	Current time
Time zone	Current time zone
Date	Current date
System free memory	Amount of unused memory in the phone
Java heap free memory	Free internal Java heap memory
Java pool free memory	Free internal Java pool memory
FIPS mode enabled	Not currently supported
Battery health	Overall health of the battery
Battery temperature	Current temperature of the battery

Field	Description
Battery level	Current battery charge level

Network Setup Web Page

The **Network Setup** page gives information about the phone and the network configuration.

Field	Description
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.
DHCP server	IP address of the Dynamic Host Configuration Protocol (DHCP) server from which the phone obtains its IP address.
BOOTP server	Not used.
DHCP	Status of DHCP use.
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 used by the phone.
DNS server 1	Primary Domain Name System (DNS) server used by the phone.
DNS server 2	Backup DNS server used by the phone.
DNS server 3	Backup DNS server used by the phone.
Alternate TFTP	Alternate Trivial File Transfer Protocol (TFTP) server. Displays Yes if enabled and No if disabled.
TFTP server 1	Primary TFTP server used by the phone.
TFTP server 2	Secondary TFTP server used by the phone.
DHCP address released	

Field	Description
Server 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 Survivable Remote Site Telephony (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.
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 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 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.
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.
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.

Field	Description
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.
Speaker enabled	Status of the speakerphone.
GARP enabled	Status of Gratuitous ARP. When enabled, the phone learns MAC addresses from Gratuitous ARP responses.
Auto line select enabled	
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 mode	Mode set for the phone.
Web access	Indicates whether access to phone web pages is enabled (Yes) or disabled (No).
SSH access enabled	Indicates if SSH access is permitted
Load server	Indicates the IP address of the load server.
CTL file	
ITL file	
ITL signature	
CAPF server	
TVS	
TFTP server	
TFTP server	
DF_BIT	Indicates the DF bit setting for packets.

Network Web Page

When you select the Network hyperlink under Network statistics, the **Port information** page displays.

Field	Description
tx bytes	Number of bytes transmitted
rx bytes	Number of bytes received
tx packets	Number of packets transmitted by the phone
rx packets	Number of packets received by the phone
tx packets dropped	
rx packets dropped	
tx packet errors	
rx packet errors	Number of error packets received by the phone
Tx frames	Number of frames transmitted
tx multicast frames	Number of multicast packets transmitted by the phone
tx retry	Number of times the phone retried and failed to send packets
tc multi retry	Number of times the phone retried to send multicast packets
tx failure	Number of transmission failures
rts success	Number of request to send (RTS) successes
rts failure	Number of request to send (RTS) failures
ack failure	Number of packet acknowledgments that failed
rx duplicate frames	Number of duplicate frames received.
rx fragmented packets	Number of fragmented packets received
Roaming count	

Console Logs Web Page

The **Console logs** page contains links to log files that Cisco TAC might need to troubleshoot problems. For instructions on how to download the logs, see Capture Phone Logs, on page 154.

Core Dumps Web Page

The **Core dumps** page contains information that Cisco TAC needs to troubleshoot problems.

Status Messages Web Page

The **Status messages** page provides a list of status messages and each message has a date and time stamp. You can use these messages to troubleshoot problems.

Debug Display Web Page

The **Debug page** shows recent messages and each message contains the date and time. You can use these messages when you troubleshoot problems.

Streaming Statistics Web Page

The phone has five **Stream** pages. All the pages have the same fields. These pages give you information about calls when you troubleshoot problems.

Table 19: Streaming Statistics Web Page Fields

Field	Description
Remote address	IP address of the caller
Local address	IP address of the phone
Start time	Timestamp for the call
Stream status	
Host name	Name of the phone
Sender packets	Number of RTP voice packets transmitted since the voice stream opened. 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 octets	Total number of octets sent by the phone.
Sender codec	Type of audio encoding sent by the phone: G.729, G.711 u-law, G.711 A-law
Sender reports sent	
Sender report time sent	
Rcvr lost packets	Number of missing RTP packets (lost in transit)
Avg jitter	Estimated average RTP packet jitter (dynamic delay that a packet encounters when going through the network).
Receiver codec	Type of audio encoding received by the phone: G.729, G.711 u-law, G.711 A-law
Receiver reports sent	Number of times this streaming statistics report has been accessed from the web page (resets when the phone resets)
Receiver report time sent	
Rcvr packets	Number of packets received by the phone
Rcvr octets	Total number of octets received by the phone.

Field	Description
Transmitter DSCP	
Receiver DSCP	
Transmitter WMM UP	
Receiver WMM UP	
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. The MOS LQK score can vary based on the type of codec that the 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
Cumulative conceal ratio	Total number of concealment frames divided by total number of speech frames received from start of the voice stream.
Interval conceal ratio	Ratio of concealment frames to speech frames in preceding 3-second interval of active speech. If using voice activity detection (VAD), a longer interval might be required to accumulate 3 seconds of active speech
Max conceal ratio	Highest interval concealment ratio from start of the voice stream.
Conceal seconds	Number of seconds that have concealment events (lost frames) from the start of the voice stream (includes severely concealed seconds)
Severely conceal seconds	Number of seconds that have more than 5 percent concealment events (lost frames) from the start of the voice stream.
Latency	
Max jitter	Maximum jitter observed since the receiving voice stream was opened.
Sender size	

Field	Description
Sender reports received	
Sender report time received	
Receiver size	
Receiver discarded	
Receiver reports received	
Receiver report time received	
Rcvr encrypted	
Sender encrypted	

CHAPTER 8

Maintenance

Reboot the Phone

You can reboot the phone to ensure that the configuration is applied to the phone.

Procedure

Step 1 Access the **Settings** app.

Step 2 Select **Admin settings** > **Reset settings** > **Reset device**.

Step 3 Press **Reset**.

Related Topics

Access the Settings App, on page 88

Boot the Phone to the Alternate Firmware

You can reboot the phone to the previous version of the phone firmware. This allows you to temporarily use the previous firmware load.

When the phone next powers on, it will use the new firmware load.

Procedure

Step 1 Press and hold **Power/End Call** ☎ until the phone turns off.

Step 2 Press and hold **Asterisk (*)** * +, and then press and hold **Power/End Call** ☎.

Step 3 When the LED changes to red, release the **Asterisk (*)** * + and **Power/End Call** ☎ keys.

The phone boots to the previous firmware version.

Restart the Phone from the Administration Web Page

You can restart the phone from the phone administration web page. Ensure that the user is not on an active call before you restart the phone.

Before you begin

Access the phone administration web page. See Access the Phone Administration Web Page, on page 92.

Procedure

Step 1 Click on the **Restart** link in the left pane.

Step 2 Click **Restart**.

Phone Reset

You can restore the factory default settings to the phone to clear the current configuration. This restore can be for all values, for the network settings, or for the security settings.

Reset the Phone to Factory Defaults from the Phone Menu

You can reset the phone to the factory defaults. The phone resets user and network setup settings to their default values and then restarts.

Procedure

Step 1 Access the **Settings** app.

Step 2 Select **Admin settings** > **Reset settings** > **All settings**.

Step 3 Press **Reset**.

Related Topics

Access the Settings App, on page 88

Reset the Phone to Factory Defaults from the Phone Keypad

You can reset the phone to factory defaults using the keypad. The phone resets user and network setup settings to their default values and then restarts.

Procedure

Step 1 Press and hold **Power/End Call** until the phone turns off.

Step 2 Press and hold **Pound (#)**, and then press and hold **Power/End Call**.

Step 3 When the LED changes to amber, release the **Pound (#)** and **Power/End Call** keys.

Step 4 Press **1 2 3 4 5 6 7 8 9 * 0 #**.

If the LED blinks green, the factory reset is in progress.

If the LED blinks red, the factory reset was not accepted.

Reset the Network Settings

You can reset the network settings on the phone to the factory defaults. The phone resets network setup settings to their default values and then restarts.

Procedure

Step 1 Access the **Settings** app.

Step 2 Select **Admin settings** > **Reset settings** > **Network settings**.

Step 3 Press **Reset**.

Related Topics

Access the Settings App, on page 88

Reset the Security Settings

You can reset the security settings on the phone to the factory defaults. The phone resets security settings to their default values and then restarts.

Procedure

Step 1 Access the **Settings** app.

Step 2 Select **Admin settings** > **Reset settings** > **Security settings**.

Step 3 Press **Reset**.

Related Topics

Access the Settings App, on page 88

Voice Quality Monitoring

To measure the voice quality of calls that are sent and received within the network, Cisco IP Phones use the following 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 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 metrics sections in the Cisco Unified Communications Manager documents.

You can access voice quality metrics on the phone or remotely by using Streaming Statistics.

Related Topics

Phone Statistics, on page 113

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 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 20: 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.
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.

Manage Core Dumps from the Admin Web Page

You can generate or delete the Java core dump log with the admin web page.

Only one core dump can be stored on the phone. The phone retains the core dump until it reboots. If a new core dump is created, the previous one is overwritten.

Before you begin

Connect to the admin web page. For more information, see Access the Phone Administration Web Page, on page 92.

Procedure

Step 1 Click **Device logs** > **Core dumps**.

Step 2 Click **Generate java core & heap dump**.

Step 3 (Optional) Click **Delete** to delete the core dump file.

CHAPTER 9

Troubleshooting

General Troubleshooting Information

The following table provides general troubleshooting information for the wireless IP phone.

Table 21: 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 Phone Reset Problems, on page 145.
Time on the phone is incorrect	Sometimes the time or date on the phone is incorrect. The 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.

Summary	Explanation
Phone firmware downgrades	After applying a Cisco Unified Communications Manager upgrade or patch, that is older than the current phone firmware, the phones could automatically downgrade to the load contained in the patch. Check the phone default image in the TFTP folder to fix this problem.
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.

Summary	Explanation
Call established with the iLBC protocol does not show that the iLBC codec is being used	Call statistics display does not show iLBC as the receiver/sender codec. 1. Check the following using 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.

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

Phone Does Not Go Through the Normal Startup Process

Problem

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

Cause

When a 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 IP Phones.
2. Verify that the wireless network is accessible:

- Power on another previously functional phone to verify that the access point is active.
- Power on the 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` is displayed on the phone screen, the battery might be dead.
   - Insert a new or fully charged battery in the phone that will not start up.
   - If you are using the battery, try plugging in the external power supply instead.
4. Reset the phone to the default settings:
   - Select **Applications** > **Admin settings** > **Reset settings** > **All settings**.
   - At the confirmation screen, select **Reset**.
5. Restart the phone from the alternate image:
   - Turn off the phone by pressing the red, power button.
   - As you press and hold *****, press the power button a second time.
   - Release ***** when the LED display changes color.

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

Connection Problems

If the phones experience connection problems that are not related to roaming, the problems are often related to the Access Point or to the way the phone connects to the Cisco Unified Communications Manager.

No Association to Wireless 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 wireless 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

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 EAP-FAST, EP-TLS, PEAP-GTC, or PEAP-MSCHAPV2 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 wireless 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.

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.

Phone Cannot Connect to TFTP Server

Problem

The TFTP server setting on the phone is incorrect.

Cause

The 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 phone may continually cycle while attempting to contact the identified TFTP server.

The 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 the TFTP server address. See Manually Set Up the Phone Network from the Settings Menu , on page 87.

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.

Phone Cannot Connect to Server

Problem

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

Solution

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

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: https://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 Manually Set Up the Phone Network from the Settings Menu , on page 87.

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: https://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a00800f0804.shtml.

Phone Cannot Connect with DNS

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 Manually Set Up the Phone Network from the Settings Menu , on page 87.

Cisco Unified Communications Manager and TFTP Services Are Not Running

Problem

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

Solution

If the Cisco Unified Communications Manager service is not running, all devices on the network that rely on it to make phone calls are affected. If the TFTP service is not running, many devices cannot start up successfully. For more information, see Start Service, on page 153.

Phone is Not Configured in Cisco Unified Communications Manager

Problem

The phone is not registered with the Cisco Unified Communications Manager

Solution

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

To verify that the phone is in the Cisco Unified Communications Manager database, choose **Device** > **Phone** from Cisco Unified Communications Manager Administration. Click **Find** to search for the phone based on the MAC Address. For information about determining a MAC address, see Determine the MAC Address of the Phone, on page 61.

If the phone is already in the Cisco Unified Communications Manager database, the configuration file may be damaged. See Configuration File Corruption, on page 145 for assistance.

Configuration File Corruption

Problem

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

Solution

Create a new phone configuration file.

Phone Reset Problems

If users report that their phones are resetting during calls or while the phones are idle, you should investigate the cause. If the network connection and Cisco Unified Communications Manager connection are stable, a phone should not reset.

Typically, a phone resets if it has problems in connecting to the network or to Cisco Unified Communications Manager.

Phone Resets Due to 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.

Phone Resets Due to 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.

Phone Resets Due to DHCP Setting Errors

Problem

The DHCP settings may be incorrect.

Solution

Verify that you have properly configured the phone to use DHCP. Verify that the DHCP server is set up properly. Verify the DHCP lease duration. We recommend that you set the lease duration to 8 days.

Related Topics

Check DHCP Settings, on page 152

Phone Resets Due to Incorrect Static IP Address

Problem

The static IP address assigned to the phone may be incorrect.

Solution

If the phone is assigned a static IP address, verify that you have entered the correct settings.

Phone Resets During Heavy Network Usage

Problem

If the phone appears to reset during heavy network usage, it is likely that you do not have a voice VLAN configured.

Solution

Isolating the phones on a separate auxiliary VLAN increases the quality of the voice traffic.

Phone Resets Due to Intentional 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 wireless phone received a command from Cisco Unified Communications Manager to reset by accessing the **Settings** app on the phone and choosing **Admin settings** > **Status** > **WLAN 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.

Phone Resets Due to DNS or Other Connectivity Issues

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 by following the procedure in Determine DNS or Connectivity Issues, on page 151.

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.

Related Topics

Roaming and Voice Quality or Lost Connection Problems, on page 149

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.

  The phone firmware supports dynamic transmit power control (DTPC). The phone uses the transmit power that the access point advertises upon association.

Note With DTPC, 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 phone is in power save mode or scanning, the access point can respond to the wireless IP phone only when ARP caching is enabled.
- 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 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

Press the **Volume** button on the side of the phone, and increase the volume.

Phone Does Not Ring

Problem

User complains that phone does not ring.

Solution

Check the phone settings:

- In the **Settings** app,
  - Check where the ringer should ring. Choose **Phone settings** > **Sounds** > **Ringer output**, and check that the correct location is selected.
  - Check the ringtone. Choose **Phone settings** > **Sounds** > **Ringtone**. If a ringtone is not set, select 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.

Feature Issues

Your users may report problems with some features. If you get the exact message that the user sees on the phone, you can identify and fix the cause of the problem.

Users Report Problems with Call Park

Problem

Your users report seeing these messages:

- `There is no free place to park this call.`
- `Call park is not available.`

Resolution

Message	Meaning
`There is no free place to park this call.`	You need to allocate more slots to park calls.
`Call park is not available.`	You have a configuration problem with Call park on your Cisco Unified Communications Manager.

For more information, see the Cisco Unified Communications Manager documentation.

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.

Related Topics

Audio Problems, on page 147

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

- Check the Neighbor List 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 wireless phone (or any wireless client) experiences roaming delays when an earlier version (SUP 1 or SUP2) blade is used.

Phone Loses Cisco Unified Communications Manager Connection While Roaming

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. Access the Neighbor list 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 32.

- If using EAP-FAST, EAP-TLS, PEAP-GTC, or PEAP-MSCHAPV2 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 Wireless IP Phone 8821 Series Deployment Guide*.

Troubleshooting Procedures

These procedures can be used to identify and correct problems.

Check TFTP Settings

Procedure

Step 1 On the Cisco IP Phone, access the Settings app, choose **Wi-Fi**, select a profile, then select **Network configuration** > **IPv4 setup** > **TFTP server 1**.

Step 2 If you have assigned a static IP address to the phone, you must manually enter a setting for the TFTP Server 1 option.

Step 3 If you are using DHCP, the phone obtains the address for the TFTP server from the DHCP server. Check that the IP address is configured in Option 150.

Step 4 You can also enable the phone to use an alternate TFTP server. Such a setting is particularly useful if the phone recently moved from one location to another.

Step 5 If the local DHCP does not offer the correct TFTP address, enable the phone to use an alternate TFTP server.

This is often necessary in VPN scenario.

Related Topics

Access the Settings App, on page 88

Determine DNS or Connectivity Issues

Procedure

Step 1 Use the Reset Settings menu to reset phone settings to their default values.

Step 2 Modify DHCP and IP settings:

a) Disable DHCP.
b) Assign static IP values to the phone. Use the same default router setting that other functioning phones use.
c) Assign a TFTP server. Use the same TFTP server that other functioning phones use.

Step 3 On the Cisco Unified Communications Manager server, verify that the local host files have the correct Cisco Unified Communications Manager server name mapped to the correct IP address.

Step 4 From Cisco Unified Communications Manager, choose **System** > **Server** and verify that reference to the server is made by the IP address and not by the DNS name.

Step 5 From Cisco Unified Communications Manager, choose **Device** > **Phone**. Click **Find** to search for this phone. Verify that you have assigned the correct MAC address to this Cisco IP Phone.

Step 6 Power cycle the phone.

Related Topics

Phone Reset, on page 132

Determine the MAC Address of the Phone, on page 61

Access the Settings App, on page 88

Check DHCP Settings

Procedure

Step 1 On the phone, access the **Settings** app.

Step 2 Select **Wi-Fi**, select the active profile, then select **Network configuration** > **IPv4 setup**, and look at the DHCP field:

- If DHCP is on, then the phone is assigned the settings from the DHCP server.
- If DHCP is off, then you must configure a static IP Address, and set the Subnet Mask, Default Router, and DNS server 1 fields.

Step 3 If you are using DHCP, check the IP addresses that your DHCP server distributes.

See the *Understanding and Troubleshooting DHCP in Catalyst Switch or Enterprise Networks* document, available at this URL:

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a00800f0804.shtml

Related Topics

Access the Settings App, on page 88

Create a New Phone Configuration File

When you remove a phone from the Cisco Unified Communications Manager database, the configuration file is deleted from the Cisco Unified Communications Manager TFTP server. The phone directory number or numbers remain in the Cisco Unified Communications Manager database. They are called unassigned DNs and can be used for other devices. If unassigned DNs are not used by other devices, delete these DNs from the Cisco Unified Communications Manager database. You can use the Route Plan Report to view and delete unassigned reference numbers. For more information, see the documentation for your particular Cisco Unified Communications Manager release.

Changing the buttons on a phone button template, or assigning a different phone button template to a phone, may result in directory numbers that are no longer accessible from the phone. The directory numbers are still assigned to the phone in the Cisco Unified Communications Manager database, but the phone has no button on the phone with which calls can be answered. These directory numbers should be removed from the phone and deleted if necessary.

Procedure

Step 1 From Cisco Unified Communications Manager, choose **Device** > **Phone** and click **Find** to locate the phone that is experiencing problems.

Step 2 Choose **Delete** to remove the phone from the Cisco Unified Communications Manager database.

Note When you remove a phone from the Cisco Unified Communications Manager database, the configuration file is deleted from the Cisco Unified Communications Manager TFTP server. The phone directory number or numbers remain in the Cisco Unified Communications Manager database. They are called unassigned DNs and can be used for other devices. If unassigned DNs are not used by other devices, delete these DNs from the Cisco Unified Communications Manager database. You can use the Route Plan Report to view and delete unassigned reference numbers.

Step 3 Add the phone back to the Cisco Unified Communications Manager database.

Step 4 Power cycle the phone.

Start Service

A service must be activated before it can be started or stopped.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Cisco Unified Serviceability** from the Navigation drop-down list and click **Go**.

Step 2 Choose **Tools** > **Control Center - Feature Services**.

Step 3 Choose the primary Cisco Unified Communications Manager server from the Server drop-down list.

The window displays the service names for the server that you chose, the status of the services, and a service control panel to start or stop a service.

Step 4 If a service has stopped, click the corresponding radio button and then click **Start**.

The Service Status symbol changes from a square to an arrow.

Capture Phone Logs

If your users have problems and you need to contact Cisco TAC for assistance, you need to capture the phone log files. The log files will help TAC resolve the problem.

Capture these logs as close to the problem event as possible. If the user can recreate the problem easily, get the user to record what they did to get the problem to occur.

Before you begin

Make sure that the web access is enabled for the phone.

If possible, ask your user for the time span that the problem occurred.

Procedure

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

a) Search for the phone in Cisco Unified Communications Manager Administration by choosing **Device** > **Phone**. Phones that register with Cisco Unified Communications Manager display the IP address on the **Find and List Phones** window and at the top of the **Phone Configuration** window.

b) On the Cisco IP Phone, access the **Settings** app, select **Phone information** > **Device information** > **Network** > **IPv4**, and then scroll to the IP Address field.

Step 2 Open a web browser and enter the following URL, where *IP_address* is the IP address of the Cisco IP Phone:

http://<IP_address>

Step 3 Click **Console logs**.

Step 4 Open the listed log files and save the files that cover the time period that the user experienced the problem.

If the problem is not limited to a specific time, save all the log files.

Related Topics

Set Up Phone Features for all Phones, on page 69
Set Up Phone Features for a Group of Phones, on page 69
Set Up Phone Features for a Single Phone, on page 70
Create a Problem Report from the Phone, on page 156

Make a Screen Capture

If your users have problems and you need to contact Cisco TAC for assistance, a capture of the phone screen may help TAC resolve the problem.

Before you begin

Make sure that the web access is enabled for the phone.

Procedure

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

a) Search for the phone in Cisco Unified Communications Manager Administration by choosing **Device** > **Phone**. Phones that register with Cisco Unified Communications Manager display the IP address on the **Find and List Phones** window and at the top of the **Phone Configuration** window.

b) On the Cisco IP Phone, access the **Settings** app, select **Phone information** > **Device information** > **Network** > **IPv4**, and then scroll to the IP Address field.

Step 2 Open a web browser and enter the following URL, where *IP_address* is the IP address of the Cisco IP Phone:

`http://`*IP_address*`/CGI/Screenshot`

Step 3 At the prompt, enter the username and password.

The phone creates an image of the phone screen.

Step 4 Save the file to your computer.

Related Topics

Set Up Phone Features for all Phones, on page 69
Set Up Phone Features for a Group of Phones, on page 69
Set Up Phone Features for a Single Phone, on page 70

Access Phone Diagnostics

The **Diagnostics** menu on the phone enables you to troubleshoot some common phone problems.

Procedure

Step 1 Access the **Settings** app.

Step 2 Select **Admin settings** > **Diagnostics**.

Perform Audio Diagnostics

The **Audio** entry in the **Diagnostics** menu on the phone enables you to troubleshoot problems with the audio on the phone.

Procedure

Step 1 Access the **Settings** app.

Step 2 Select **Admin settings** > **Diagnostics** > **Audio**.

Step 3 Listen to the tone on the handset speaker.

Step 4 Press the **Speaker** button to turn on handsfree, and listen to the tone.

Step 5 Plug in a wired headset and listen to the tone.

Perform WLAN Diagnostics

The **WLAN** entry in the **Diagnostics** menu on the phone enables you to troubleshoot WLAN problems from the phone.

Procedure

Step 1 Access the **Settings** app.

Step 2 Select **Admin settings** > **Diagnostics** > **WLAN**.

Step 3 At the prompt, select **Continue**.

Step 4 Select the profile that is currently in use.

The screen displays the WLAN information.

Find the List of Neighbor Access Points

The Neighbor list menu on the phone gives you the list of access points that the phone can connect to.

Procedure

Step 1 Access the **Settings** app.

Step 2 Select **Admin settings** > **Neighbor list**.

Related Topics

Access the Settings App, on page 88

Create a Problem Report from the Phone

If your users have a problem with their phones, you can ask them to generate a problem report using the problem report tool (PRT). You can access the report from the phone administration web page.

Procedure

Step 1 On the phone that has the problem, access the **Settings** app.

Step 2 Select **Phone information** > **Report problem**.

Step 3 Press **Submit**.

Step 4 Access the phone administration web page to download the report.

Related Topics

Cisco IP Phone Administration Page, on page 91

Access the Settings App, on page 88

Generate a Problem Report from the Admin Web Page

You can remotely generate a problem report for a phone with the admin web page.

Before you begin

Connect to the admin web page. For more information, see Access the Phone Administration Web Page, on page 92.

Procedure

Step 1 Click **Device logs** > **Console logs**.

Step 2 Click **Report problem**.

CHAPTER 10

International User Support

Unified Communications Manager Endpoints Locale Installer

By default, Cisco IP Phones are set up for the English (United States) locale. To use the Cisco IP Phones in other locales, you must install the locale-specific version of the Unified Communications Manager Endpoints Locale Installer on every Cisco Unified Communications Manager server in the cluster. The Locale Installer installs the latest translated text for the phone user interface and country-specific phone tones on your system so that they are available for the Cisco IP Phones.

To access the Locale Installer required for a release, access https://software.cisco.com/download/navigator.html?mdfid=286037605&flowid=46245, navigate to your phone model, and select the Unified Communications Manager Endpoints Locale Installer link.

For more information, see the documentation for your particular Cisco Unified Communications Manager release.

Note The latest Locale Installer may not be immediately available; continue to check the website for updates.

International Call Logging Support

If your phone system is configured for international call logging (calling party normalization), the call logs, redial, or call directory entries may display a plus (+) symbol to represent the international escape code for your location. Depending on the configuration for your phone system, the + may be replaced with the correct international dialing code, or you may need to edit the number before dialing to manually replace the + with the international escape code for your location. In addition, while the call log or directory entry may display the full international number for the received call, the phone display may show the shortened local version of the number, without international or country codes.

Language Limitation

There is no localized Keyboard Alphanumeric Text Entry (KATE) support for the following Asian locales:

- Chinese (China)
- Chinese (Hong Kong)
- Chinese (Taiwan)
- Japanese (Japan)
- Korean (Korea Republic)

The default English (United States) KATE is presented to the user instead.

For example, the phone screen will show text in Korean, but the **2** key on the keypad will display **`a b c 2 A B C`**.

CHAPTER 11

Technical Specifications

Physical and Operating Environment

The following table shows the physical and operating environment specifications for the Cisco Wireless IP Phone 8821 and 8821-EX.

Table 22: Physical and Operating Specifications

Specification	**8821** **Value or Range**	**8821-EX** **Value or Range**
Operating temperature	14° to 122°F (-10° to 50°C)	14° to 122°F (-10° to 50°C)
Operating relative humidity	Operating: 10% to 95% (non-condensing) Non-operating: 10% to 95% (non-condensing)	10% to 95% (noncondensing)
Storage temperature	-22° to 140°F (–30° to 60°C)	-22° to 140°F (–30° to 60°C)
Drop Specification	5 ft (1.5 m) to concrete without carrying case	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	-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	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

Specification	8821 Value or Range	8821-EX Value or Range
Altitude	Certified for operation from 0 to 6500 ft (0 to 2 km)	Certified for operation from 0 to 6500 ft (0 to 2 km)
Endurance	IP54 MIL-STD-810G Drop and Vibration procedures	IP54 MIL-STD-810G Drop and Vibration procedures
Phone width	2.2 inches (55.88 mm)	
Phone length	5.2 inches (132.08 mm)	
Phone depth	0.7 inches (17.78 mm)	
Phone weight	phone: 121 grams battery: 37 grams total: 158 grams	
LCD	2.4-inch (6-cm), 320x240 color display	
Power	AC adapters by geographic region Rechargeable Lithium ion 4.35V, 2060mAh smart battery	

For more information, see the phone datasheets, located at https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/datasheet-listing.html.

Bluetooth Technology

The Cisco Wireless IP Phone 882x Series are full-feature telephones 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 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 23: 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 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 wireless IP phones. The phones support the Hands-Free Profile Version 1.5.

Because of potential interference issues, we recommend 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 phone on the same side of the body as the Bluetooth-enabled headset.

⚠

Caution The Cisco Wireless IP Phone 8821-EX has not been tested or certified to use any Bluetooth accessories in hazardous environments.

For information about pairing headsets, see Headset Usage, on page 163.

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

Headset Usage

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

⚠

Caution The Cisco Wireless IP Phone 8821-EX has not been tested or certified to use any Bluetooth accessories, including headsets, 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.

The primary reason that a particular headset would be inappropriate for the 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 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 phone users.

Related Topics

External Devices

CHAPTER 12

Product Safety and Security

Safety and Performance Information

Read the following safety notices before installing or using your IP phone.

Warning 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

To see translations of the warnings that appear in this publication, refer to the statement number in the *Regulatory Compliance and Safety Information—Cisco Wireless IP Phone 882x Series* at the following URL: http://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cuipph/882x/english/RCSI/RCSI-0266-book.pdf

Warning Read the installation instructions before using, installing, or connecting the system to the power source. Statement 1004

Warning Voice over IP (VoIP) service and the emergency calling service do not function if power fails or is disrupted. After power is restored, you might have to reset or reconfigure equipment to regain access to VoIP and the emergency calling service. In the USA, this emergency number is 911. You need to be aware of the emergency number in your country. Statement 361

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

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

Safety Guidelines

The following are safety guidelines for using the Cisco Wireless IP Phone 8821 and 8821-EX in specific environments:

- Do not use this product as the primary communications tool in healthcare environments, as it may use an unregulated frequency band that is susceptible to interference from other devices or equipment.
- The use of wireless devices in hospitals is restricted to the limits set forth by each hospital.
- The use of wireless devices in hazardous locations is limited to the constraints posed by the safety directors of such environments.
- The use of wireless devices on airplanes is governed by the Federal Aviation Administration (FAA).

Battery Safety Notices

These battery safety notices apply to the batteries that are approved for the Cisco Wireless IP Phone 8821 and 8821-EX.

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

Warning Do not touch or bridge the metal contacts on the battery. Unintentional discharge of the batteries can cause serious burns. Statement 341

Warning Explosion Hazard: Do not charge the phone battery in a potentially explosive environment. Statement 431

Warning Lithium ion batteries have limited lifetimes. Any lithium ion battery that shows any signs of damage, including swelling, should be properly discarded immediately.

⚠

Caution

- Do not dispose of the battery pack in fire or water. The battery may explode if placed in a fire.
- Do not disassemble, crush, puncture, or incinerate the battery pack.
- 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.
- Do not charge the battery pack if the ambient temperature exceeds 104 degrees Fahrenheit (40 degrees Celsius).
- Do not expose the battery pack to high storage temperatures (above 140 degrees Fahrenheit, 60 degrees Celsius).
- When discarding a battery pack, contact your local waste disposal provider regarding local restrictions on the disposal or recycling of batteries.

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

Battery

CP-BATT-8821=

Use only the Cisco b that is compatible with your phone. To order your power supply, contact your local dealer and refer to the list of Cisco part numbers.

Argentina

CP-PWR-8821-AR=

Australia

CP-PWR-8821-AU=

Brazil

CP-PWR-8821-BZ=

Europe

CP-PWR-8821-CE=

Korea

CP-PWR-8821-KR=

Japan

CP-PWR-8821-JP=

Switzerland

CP-PWR-8821-SW=

North America

CP-PWR-8821-NA=

United Kingdom

CP-PWR-8821-UK=

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

Hazardous Environments

The Cisco Wireless IP Phone 8821-EX is ATEX Class I Zone 2 and CSA Class I Division 2/Zone 2 certified equipment. This means the phone can be operated in 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.

Warning Explosion Hazard—Do not charge the phone battery in a potentially explosive atmosphere. Statement 431

Warning Explosion Hazard—Substitution of components may impair suitability for class1, Division 2/Zone 2. Statement 1083

Power Outage

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

Regulatory Domains

The radio frequency (RF) for this phone is configured for a specific regulatory domain. If you use this phone outside of the specific regulatory domain, the phone will not function properly, and you might violate local regulations.

Health-Care Environments

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

External Devices Usage

The following information applies when you use external devices with the wireless phone.

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

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

- Move the external device away from the source of the RF or AF signals.
- Route the external device cables away from the source of the RF or AF signals.
- Use shielded cables for the external device, or use cables with a better shield and connector.
- Shorten the length of the external device cable.
- Apply ferrites or other such devices on the cables for the external device.

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

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

Phone Behavior During Times of Network Congestion

Anything that degrades network performance can affect phone audio and, in some cases, can cause a call to drop. Sources of network degradation can include, but are not limited to, the following activities:

- Administrative tasks, such as an internal port scan or security scan
- Attacks that occur on your network, such as a Denial of Service attack

SAR

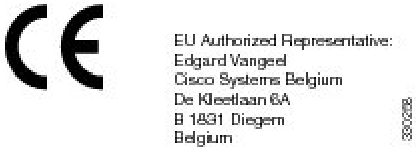
	This product meets applicable national SAR limits of 1.6W/kg. The specific maximum SAR values can be found in Compliance Statements, on page 170. When carrying the product or using it while worn on your body, either use an approved accessory such as a holster or otherwise maintain a distance of 5 mm from the body to ensure compliance with RF exposure requirements. Note that the product may be transmitting even if you are not making a phone call.

Compliance Statements

Compliance Statements for the European Union

CE Marking

The following CE mark is affixed to the equipment and packaging.



EU Authorized Representative:
Edgard Vangeel
Cisco Systems Belgium
De Kleetlaan 6A
B 1831 Diegem
Belgium

RF Exposure Statement for the European Union

This device has been evaluated and found compliant in accordance with EU EMF Directive 2014/53/EU.

Compliance Statements for the USA

SAR Statement

The Cisco Wireless IP Phone 882x Series handsets have been tested for body-worn Specific Absorption Rate (SAR) compliance using the specific belt-clip/holster configuration provided with the handset. The FCC has established the detailed body-worn SAR requirements and has established that these requirements have been met with the specific belt-clip/holster provided with the handset. Other belt-clip/holsters or similar accessories that have not been tested may not comply and therefore should be avoided.

RF Exposure Information

The radio module has been evaluated found to be compliant to the requirements as set forth in 47 CFR Sections 2.1091, 2.1093, and 15.247 (b) (4) addressing RF Exposure from radio frequency devices. This model meets the applicable government requirements for exposure to radio frequency waves.

THIS DEVICE MEETS THE LIMITS AS REFERENCED BY ISED RSS-102 R5 FOR EXPOSURE TO RADIO WAVES

Your Cisco Wireless IP Phone 882x Series device includes a radio transmitter and receiver. It is designed not to exceed the General populace (uncontrolled) limits for exposure to radio waves (radio frequency electromagnetic fields) as referenced in RSS-102 which references Health Canada Safety Code 6 and include a substantial safety margin designed to assure the safety of all persons, regardless of age and health.

As such the systems are designed to be operated as to avoid contact with the antennas by the end user. It is recommended to set the system in a location where the antennas can remain at least a minimum distance as specified from the user in accordance to the regulatory guidelines which are designed to reduce the overall exposure of the user or operator.

The device has been tested and found compliant with the applicable regulations as part of the radio certification process.

Maximum SAR for this Model and Conditions Under Which it was Recorded		
Head SAR	WLAN 5GHz	0.63 W/kg
Body-worn SAR	WLAN 5GHz	0.67 W/kg

This wireless phone contains a radio transceiver. The radio transceiver and antenna have been designed to meet the RF emission requirements for human exposure as specified by the FCC as well as by other agencies from other countries. These guidelines were developed by the industry based on guidance from the World Health Organization (WHO). These industry standards have been developed to include additional safety margins to ensure that the user is exposed to the least amount of RF radiation.

The radio transceiver uses a non ionization type of radiation as opposed to an ionized radiation such as an X-Ray wave.

The exposure standard for these devices references a unit of measure known as SAR. The limit as set by the FCC is 1.6W/kg. The tests for this emission level is done in an independent laboratory who employs test methods and operating positions reviewed by the FCC and other agencies.

Before the phone was placed on the market, the product was tested and certified in accordance with the FCC regulations to verify that the product did not exceed the FCC SAR requirements.

Additional information on SAR and RF Exposure can be obtained off the FCC website at: http://www.fcc.gov/oet/rfsafety

There is no conclusive proof that these mobile phones are or are not a health risk. The FDA and numerous researchers are continuing studies of RF radiation and health issues. Additional information on this subject can be obtained from the FDA web site at: http://www.fda.gov

The Cisco Wireless IP Phone 882x Series operates at power levels that are 5 to 6 times lower than most standard cellular, Personal Communications Service (PCS), or Global System for Mobile Communication (GSM) phones. This lower power coupled with a lower transmitter duty cycle reduces the user’s exposure to the RF fields.

There are several suggested methods to reduce exposure for the user. Among those include:

1. Using a hands-free handset to increase the distance between the antenna and the head of the user.
2. Orienting the antenna away from the user.

Additional information can be obtained from the following documentation:

- Cisco Systems Spread Spectrum Radios and RF Safety white paper at the following location: http://www.cisco.com/warp/public/cc/pd/witc/ao340ap/prodlit/rfhr_wi.htm
- FCC Bulletin 56: Questions and Answers about Biological Effects and Potential Hazards of Radio Frequency Electromagnetic Fields
- FCC Bulletin 65: Evaluating Compliance with the FCC guidelines for Human Exposure to Radio Frequency Electromagnetic Fields

Additional information can also be obtained from the following organizations:

- World Health Organization Internal Commission on Non-Ionizing Radiation Protection at http://www.who.int/emf
- United Kingdom, National Radiological Protection Board at http://www.nrpb.org.uk

- Cellular Telecommunications Association at http://www.wow-com.com

General RF Exposure Compliance

This device has been evaluated and found compliant to the ICNIRP (International Committee on Non-Ionizing Radiation Protection) limits for Human Exposure of RF Exposure.

Part 15 Radio Device

⚠

Caution The Part 15 radio device operates on a non-interference basis with other devices operating at this frequency. Any changes or modification to said product not expressly approved by Cisco, including the use of non-Cisco antennas, could void the user’s authority to operate this device.

Compliance Statements for Canada

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device. Privacy of communications may not be ensured when using this phone.

This product meets the applicable Innovation, Science and Economic Development Canada technical specifications.

Avis de Conformité Canadien

Cet appareil est conforme aux normes RSS exemptes de licence RSS d’Industry Canada. Le fonctionnement de cet appareil est soumis à deux conditions : (1) ce périphérique ne doit pas causer d'interférence et (2) ce périphérique doit supporter les interférences, y compris celles susceptibles d'entraîner un fonctionnement non souhaitable de l'appareil. La protection des communications ne peut pas être assurée lors de l'utilisation de ce téléphone.

Le présent produit est conforme aux spécifications techniques applicables d'Innovation, Sciences et Développement économique Canada.

Canadian RF Exposure Statement

THIS DEVICE MEETS THE LIMITS AS REFERENCED BY ISED RSS-102 R5 FOR EXPOSURE TO RADIO WAVES

Your device includes a radio transmitter and receiver. It is designed not to exceed the General populace (uncontrolled) limits for exposure to radio waves (radio frequency electromagnetic fields) as referenced in RSS-102 which references Health Canada Safety Code 6 and include a substantial safety margin designed to assure the safety of all persons, regardless of age and health.

As such the systems are designed to be operated as to avoid contact with the antennas by the end user. It is recommended to set the system in a location where the antennas can remain at least a minimum distance as specified from the user in accordance to the regulatory guidelines which are designed to reduce the overall exposure of the user or operator.

The device has been tested and found compliant with the applicable regulations as part of the radio certification process.

Maximum SAR for this Model and Conditions Under Which it was Recorded		
Head SAR	WLAN 5GHz	0.63 W/kg
Body-worn SAR	WLAN 5GHz	0.67 W/kg

Déclaration d'Exposition aux RF Canadienne

CE PÉRIPHÉRIQUE RESPECTE LES LIMITES DÉCRITES PAR LA NORME RSS-102 R5 D'EXPOSITION À DES ONDES RADIO

Votre appareil comprend un émetteur et un récepteur radio. Il est conçu pour ne pas dépasser les limites applicables à la population générale (ne faisant pas l'objet de contrôles périodiques) d'exposition à des ondes radio (champs électromagnétiques de fréquences radio) comme indiqué dans la norme RSS-102 qui sert de référence au règlement de sécurité n°6 sur l'état de santé du Canada et inclut une marge de sécurité importantes conçue pour garantir la sécurité de toutes les personnes, quels que soient leur âge et état de santé.

En tant que tels, les systèmes sont conçus pour être utilisés en évitant le contact avec les antennes par l'utilisateur final. Il est recommandé de positionner le système à un endroit où les antennes peuvent demeurer à au moins une distance minimum préconisée de l'utilisateur, conformément aux instructions des réglementations qui sont conçues pour réduire l'exposition globale de l'utilisateur ou de l'opérateur.

Le périphérique a été testé et déclaré conforme aux réglementations applicables dans le cadre du processus de certification radio.

DAS maximal pour ce modèle et conditions dans lesquelles il a été enregistré		
DAS au niveau de la tête	WLAN 5GHz	0.63 W/kg
DAS près du corps	WLAN 5GHz	0.67 W/kg

Compliance Statements for New Zealand

Permit to Connect (PTC) General Warning

The grant of a Telepermit for any item of terminal equipment indicates only that Telecom has accepted that the item complies with minimum conditions for connection to its network. It indicates no endorsement of the product by Telecom, nor does it provide any sort of warranty. Above all, it provides no assurance that any item will work correctly in all respects with another item of Telepermitted equipment of a different make or model, nor does it imply that any product is compatible with all of Telecom's network services.

Use of IP Networks with the PSTN

Internet Protocol (IP) by its nature introduces delay into speech signals as each data packet is formulated and addressed. Telecom Access Standards recommends that suppliers, designers and installers using this technology for calls to or from the PSTN refer to ITU E Model requirements in the design of their networks. The overall aim is to minimise delay, distortion and other transmission impairments, particularly for those calls involving cellular and international networks, which already suffer extensive delay.

The Use of Voice Compression Through the PSTN

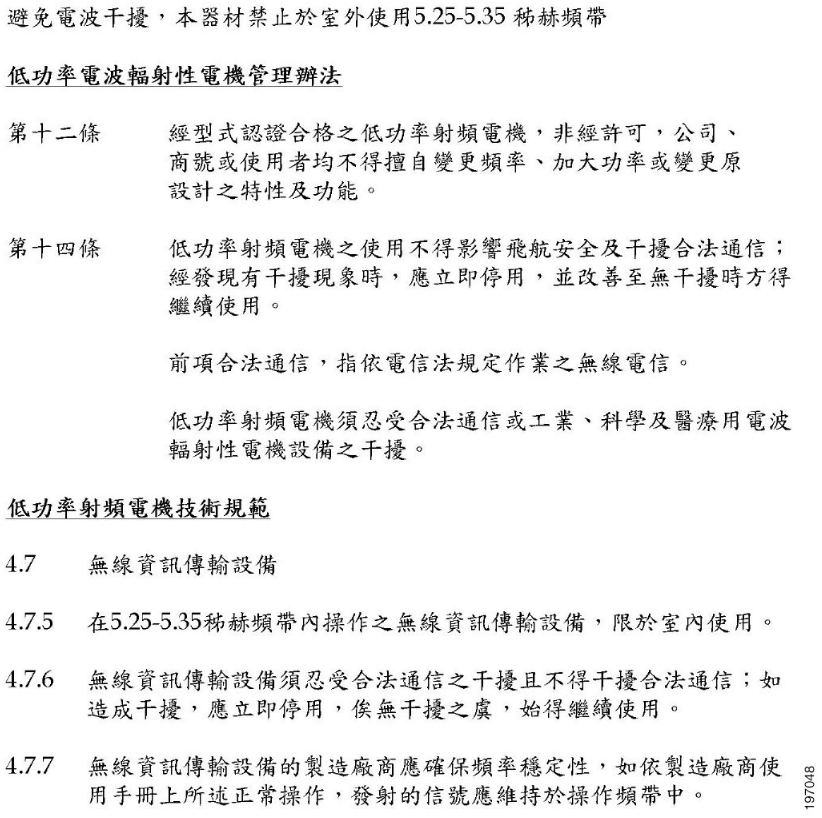
Because of the extensive delay already experienced when calling cellular and international networks, some of which is already caused by their use of voice compression technologies. Telecom Access Standards will only approve G711 voice technology for use on the PSTN. G711 is an ‘instantaneous speech-encoding technique’ whereas G729 and all its variants are considered ‘near instantaneous’ introducing additional delay into the speech signal.

Echo Cancellation

Echo cancelers are not normally required in the Telecom PSTN because geographic delays are acceptable where CPE return loss is maintained within Telepermit limits. However, those private networks that make use of Voice-over-IP (VoIP) technology are required to provide echo cancellation for all voice calls. The combined effect of audio/VoIP conversion delay and IP routing delay can cause the echo cancellation time of 64 mS to be required.

Compliance Statements for Taiwan

DGT Warning Statement



避免電波干擾，本器材禁止於室外使用5.25-5.35 秭赫頻帶

低功率電波輻射性電機管理辦法

第十二條　經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條　低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。

前項合法通信，指依電信法規定作業之無線電信。

低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

低功率射頻電機技術規範

4.7　無線資訊傳輸設備

4.7.5　在5.25-5.35秭赫頻帶內操作之無線資訊傳輸設備，限於室內使用。

4.7.6　無線資訊傳輸設備須忍受合法通信之干擾且不得干擾合法通信；如造成干擾，應立即停用，俟無干擾之虞，始得繼續使用。

4.7.7　無線資訊傳輸設備的製造廠商應確保頻率穩定性，如依製造廠商使用手冊上所述正常操作，發射的信號應維持於操作頻帶中。

Compliance Statement for Argentina

Advertencia

No utilizar una fuente de alimentación con caracteristícas distintas a las expresadas ya que podría ser peligroso.

Compliance Statements for Brazil

Art. 6º - 506

This equipment is a secondary type device, that is, it is not protected against harmful interference, even if the interference is caused by a device of the same type, and it also cannot cause any interference to primary type devices.

For more information, go to this URL: http://www.anatel.gov.br

Este equipamento opera em caráter secundário, isto é, não tem direito a proteção contra interferência prejudicial, mesmo de estações do mesmo tipo, e não pode causar interferência a sistemas operando em caráter primário.

Site Anatel: http://www.anatel.gov.br

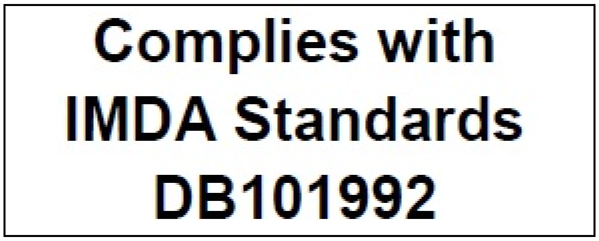
Resolution nº 303/2002 e nº 533/2009

This product is approved by Anatel, in accordance with the procedures regulated by Resolution no. 242/2000 and meets the technical requirements applied, including the exposure limits of the Specific Absorption Rate for electric, magnetic and electromagnetic fields of radiofrequency, in accordance with Resolutions nº 303/2002 and nº 533/2009.

Resoluções no. 303/2002 e no. 533/2009

Este produto está homologado pela Anatel, de acordo com os procedimentos regulamentados pela Resolução no. 242/2000 e atende aos requisitos técnicos aplicados, incluindo os limites de exposição da Taxa de Absorção Específica referente a campos elétricos, magnéticos e eletromagnéticos de radiofrequência, de acordo com as Resoluções no. 303/2002 e no. 533/2009.

Compliance Statement for Singapore



Complies with
IMDA Standards
DB101992

Cisco Product Security Overview

This product contains cryptographic features and is subject to U.S. and local country laws that govern 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 can be found at https://www.bis.doc.gov/policiesandregulations/ear/index.htm.

Important Online Information

End User License Agreement

The End User License Agreement (EULA) is located here: https://www.cisco.com/go/eula

Regulatory Compliance and Safety Information

Regulatory Compliance and Safety Information (RCSI) is located here: