Cisco IP Conference Phone 8832 Administration Guide for Cisco Unified Communications Manager

First Published: 2017-09-15

Last Modified: 2023-06-16

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.

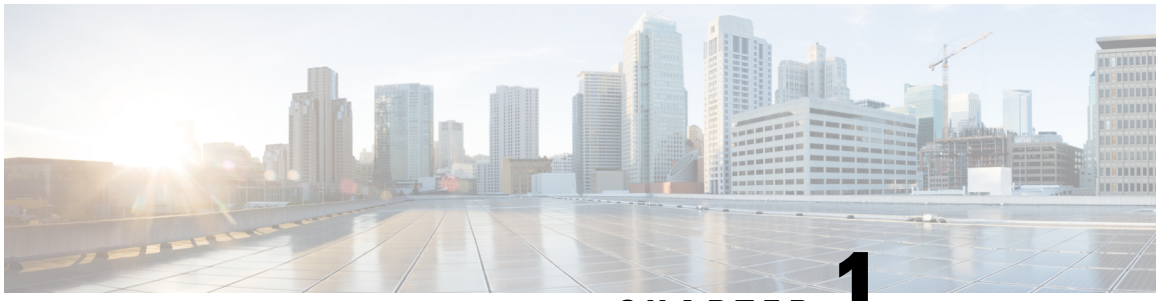
All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

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

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

CONTENTS



CHAPTER 1

New and Changed Information

New and Changed Information for Firmware Release 14.2(1)

The following information is new or changed for Firmware Release 14.2(1).

Feature	New or Changed
Support for SIP OAuth on SRST	Security Enhancements for Your Phone Network, on page 72

New and Changed Information for Firmware Release 14.1(1)

The following information is new or changed for Firmware Release 14.1(1).

Feature	New or Changed
SIP OAuth for Proxy TFTP support	Security Enhancements for Your Phone Network, on page 72
Phone Migration without Transition Load	Migration of your Phone to a Multiplatform Phone Directly, on page 93

New and Changed Information for Firmware Release 14.0(1)

Table 1: New and Changed Information

Feature	New or Changed
Call Park Monitoring Enhancement	Product Specific Configuration, on page 97
SIP OAuth Enhancements	Security Enhancements for Your Phone Network, on page 72
OAuth Enhancements for MRA	Mobile and Remote Access Through Expressway, on page 117
User Interface Enhancements	Survivable Remote Site Telephony, on page 64

As of Firmware Release 14.0, the phones support DTLS 1.2. DTLS 1.2 requires Cisco Adaptive Security Appliance (ASA) Release 9.10 or later. You configure the minimum DTLS version for a VPN connection in ASA. For more information, see *ASDM Book 3: Cisco ASA Series VPN ASDM Configuration Guide* at https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html

New and Changed Information for Firmware Release 12.8(1)

The following information is new or changed for Firmware Release 12.8(1).

Feature	New or Changed Content
Phone Data Migration	Change a User's Phone Model, on page 52
Add additional information about the Web Access field	Product Specific Configuration, on page 97

New and Changed Information for Firmware Release 12.7(1)

No administration guide updates were required for Firmware Release 12.7(1).

New and Changed Information for Firmware Release 12.6(1)

No administration guide updates were required for Firmware Release 12.6(1).

New and Changed Information for Firmware Release 12.5(1)SR3

All references to the Cisco Unified Communications Manager documentation have been updated to support all Cisco Unified Communications Manager releases.

Table 2: Cisco IP Phone 8832 Administration Guide Revisions for Firmware Release 12.5(1)SR3

Revision	Updated Section
Support for Activation Code Onboarding and Mobile and Remote Access	Activation Code Onboarding and Mobile and Remote Access, on page 29
Support for the Problem Report Tool use from Cisco Unified Communications Manager.	Create a Phone Problem Report from Cisco Unified Communications Manager, on page 165

New and Changed Information for Firmware Release 12.5(1)SR2

No administration guide updates were required for Firmware Release 12.5(1)SR2.

Firmware Release 12.5(1)SR2 replaces Firmware Release 12.5(1) and Firmware 12.5(1)SR1. Firmware Release 12.5(1) and Firmware Release 12.5(1)SR1 have been deferred in favor of Firmware Release 12.5(1)SR2.

New and Changed Information for Firmware Release 12.5(1)SR1

The following table lists the changes made to the *Cisco IP Conference Phone 8832 Administration Guide for Cisco Unified Communications Manager* to support Firmware Release 12.5(1)SR1.

Table 3: Cisco IP Conference Phone 8832 Administration Guide Revisions for Firmware Release 12.5(1)SR1

Revision	New or Updated Section
Support for Elliptic Curve	Supported Security Features, on page 73

New and Changed Information for Firmware Release 12.5(1)

The following table lists the changes made to the *Cisco IP Conference Phone 8832 Administration Guide for Cisco Unified Communications Manager* to support Firmware Release 12.5(1).

Table 4: Cisco IP Conference Phone 8832 Administration Guide Revisions for Firmware Release 12.5(1)

Revision	New or Updated Section
Support for Whisper Paging on Cisco Unified Communications Manager Express	Cisco Unified Communications Manager Express Interaction, on page 22
Support for Disable TLS Ciphers	Product Specific Configuration, on page 97

Revision	New or Updated Section
Support for Enbloc Dialing for Inter-Digit Timer T.302 Enhancement.	Product Specific Configuration, on page 97

New and Changed Information for Firmware Release 12.1(1)

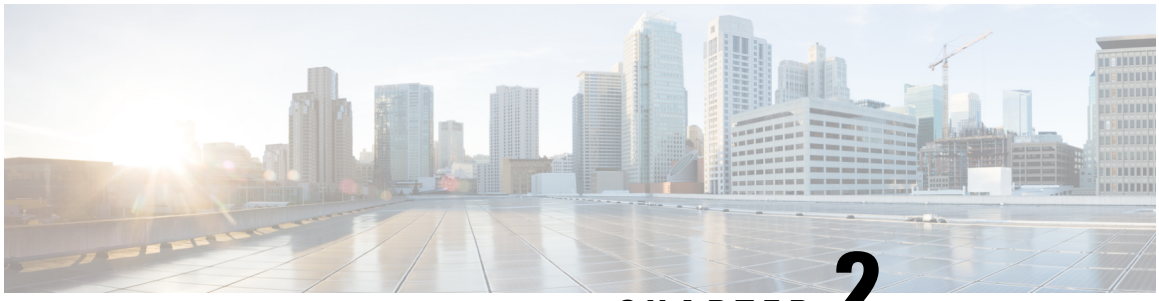
The following table describes changes to the *Cisco IP Conference Phone 8832 Administration Guide for Cisco Unified Communications Manager* to support Firmware Release 12.1(1).

Revision	New or Updated Section
Support for Cisco IP Conference Phone 8832 PoE Injector	• Phone Power Requirements, on page 18 • Ways to Provide Power to Your Conference Phone, on page 32 • Install the Conference Phone, on page 31
Support for Wireless Microphones	• Cisco IP Conference Phone 8832, on page 9 • Wireless Expansion Microphone (8832 Only), on page 13 • Install the Wireless Expansion Microphones, on page 36 • Install the Wireless Microphone Charging Cradle, on page 37
Support for Daisy Chain	• Cisco IP Conference Phone 8832, on page 9 • Daisy Chain Mode, on page 31 • Install the Conference Phone in Daisy Chain Mode, on page 38 • One Phone in Daisy Chain Mode Doesn't Work, on page 163
Support for Cisco IP Conference Phone 8832 Non-PoE Ethernet Injector	• Install the Conference Phone, on page 31 • Ways to Provide Power to Your Conference Phone, on page 32

Revision	New or Updated Section
Support for Wi-Fi	• Install the Conference Phone, on page 31 • Ways to Provide Power to Your Conference Phone, on page 32 • Set Domain Name Field, on page 46 • Enable Wireless LAN from the Phone, on page 46 • Set Up the Wireless LAN from Cisco Unified Communications Manager, on page 47 • Set Up Wireless LAN from the Phone, on page 48 • Set the Number of WLAN Authentication Attempts, on page 49 • Enable WLAN Prompt Mode, on page 50 • Set Up a Wi-Fi Profile using Cisco Unified Communications Manager, on page 50 • Set Up a Wi-Fi Group using Cisco Unified Communications Manager, on page 52
Support for Mobile and Remote Access Through Expressway	• Mobile and Remote Access Through Expressway, on page 117 • Deployment Scenarios, on page 118 • Configure User Credentials Persistent for Expressway Sign-In, on page 119
Support for enabling or disabling TLS 1.2 for web server access.	Product Specific Configuration, on page 97
Support for G722.2 AMR-WB audio codec	• Cisco IP Conference Phone 8832, on page 9 • Call Statistics Fields, on page 136

PART I

About the Cisco IP Conference Phone



CHAPTER 2

Cisco IP Conference Phone Hardware

Cisco IP Conference Phone 8832

The Cisco IP Conference Phone 8832 and 8832NR enhance people-centric communications. It combines superior high-definition (HD) audio performance and 360-degree coverage for medium to large conference rooms and executive offices. It provides an audiophile sound experience with a full-duplex two-way wideband (G.722) audio hands-free speaker. This phone is a simple solution that meets the challenges of the most diverse rooms.

Figure 1: Cisco IP Conference Phone 8832

The conference phone has sensitive microphones with 360-degree coverage. This coverage lets you speak in a normal voice and be heard clearly from up to 10 feet (3 m) away. The phone also features technology that resists interference from mobile phones and other wireless devices, which assures delivery of clear communications without distractions. The phone provides a color screen and softkey buttons to access user

functions. With the base unit alone, the phone provides coverage for a 20 x 20 ft. (6.1 x 6.1 m) room and up to 10 people.

Two wired expansion microphones are available for use with the phone. Placing the expansion microphones away from the base unit provides greater coverage in larger conference rooms. With the base unit and wired expansion microphones, the conference phone provides coverage for a 20 x 34 ft. (6.1 x 10 m) room and up to 22 people.

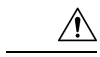
The phone also supports an optional set of two wireless expansion microphones. With the base unit and wireless expansion microphones, the conference phone provides coverage for a 20 x 40 ft. (6.1 x 12.2 m) room and up to 26 people. To cover a 20 x 40 ft. room, we recommend that you place each microphone at a maximum distance of 10 ft. from the base.

You can connect two base units to increase the coverage for a room. This configuration requires the optional Daisy Chain kit and can support two expansion microphones (either wired or wireless, but not a mixed combination). If you are using wired microphones with the Daisy Chain kit, the configuration provides coverage for a room up to 20 x 50 feet (6.1 x 15.2 m) and up to 38 people. If you are using wireless microphones with the Daisy Chain kit, the configuration provides coverage for a room up to 20 x 57 feet (6.1 x 17.4 m) and up to 42 people.

The Cisco IP Conference Phone 8832NR (non-radio) version does not support Wi-Fi, wireless expansion microphones, or Bluetooth.

Like other devices, a Cisco IP Phone must be configured and managed. These phones encode and decode the following codecs:

- G.711 a-law
- G.711 mu-law
- G.722
- G722.2 AMR-WB
- G.729a/G.729ab
- G.726
- iLBC
- Opus



Caution Using a cell, mobile, or GSM phone, or two-way radio in close proximity to a Cisco IP Phone might cause interference. For more information, see the manufacturer's documentation of the interfering device.

Cisco IP Phones provide traditional telephony functionality, such as call forwarding and transferring, redialing, speed dialing, conference calling, and voice messaging system access. Cisco IP Phones also provide a variety of other features.

As with other network devices, you must configure Cisco IP Phones to prepare them to access Cisco Unified Communications Manager and the rest of the IP network. By using DHCP, you have fewer settings to configure on a phone. If your network requires it, however, you can manually configure information such as: an IP address, TFTP server, and subnet information.

Cisco IP Phones can interact with other services and devices on your IP network to provide enhanced functionality. For example, you can integrate Cisco Unified Communications Manager with the corporate

Lightweight Directory Access Protocol 3 (LDAP3) standard directory to enable users to search for coworker contact information directly from their IP phones. You can also use XML to enable users to access information such as weather, stocks, quote of the day, and other web-based information.

Finally, because the Cisco IP Phone is a network device, you can obtain detailed status information from it directly. This information can assist you with troubleshooting any problems users might encounter when using their IP phones. You can also obtain statistics about an active call or firmware versions on the phone.

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

Cisco IP Conference Phone 8832 Buttons and Hardware

The following figure shows the Cisco IP Conference Phone 8832.

Figure 2: Cisco IP Conference Phone 8832 Buttons and Features

The following table describes the buttons on the Cisco IP Conference Phone 8832.

Table 5: Cisco IP Conference Phone 8832 Buttons

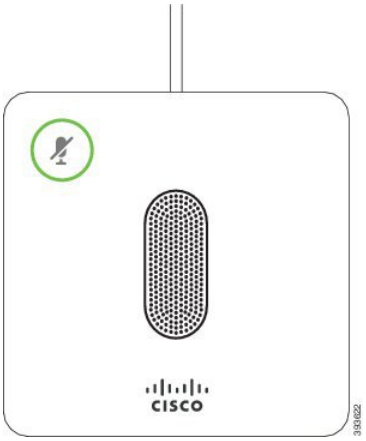
1	LED bar	Indicates call states: • Green, solid—Active call • Green, flashing—Incoming call • Green, pulsing—Held call • Red, solid—Muted call

2	Expansion microphone port	The wired expansion microphone cable plugs into the port.
3	**Mute** bar	Toggles the microphone on or off. When you mute the microphone, the LED bar lights red.
4	Softkey buttons	Access functions and services.
5	Navigation bar and **Select** button	Scroll through menus, highlight items, and select the highlighted item.
6	**Volume** button	Adjusts the speakerphone volume (off hook) and the ringer volume (on hook). When you change the volume, the LED bar lights white to show the volume change.

Wired Expansion Microphone (8832 Only)

The Cisco IP Conference Phone 8832 supports two wired expansion microphones, available in an optional kit. Use the expansion microphones in larger rooms or in a crowded room. For best results, we recommend that you place the microphones between 3 feet (0.91 m) and 7 feet (2.1 m) away from the phone.

Figure 3: Wired Expansion Microphone



When you're in a call, the expansion microphone LED around the **Mute** button is green.

When you mute the microphone, the LED is red. When you press the **Mute** button, the phone and the expansion microphones are muted.

Related Topics

Install the Wired Expansion Microphones, on page 35

Wireless Expansion Microphone (8832 Only)

The Cisco IP Conference Phone 8832 supports two expansion wireless microphones, available with a charging cradle in an optional kit. When the wireless microphone is placed on the charging cradle for charging, the LED on the cradle is lit white.

Figure 4: Wireless Microphone

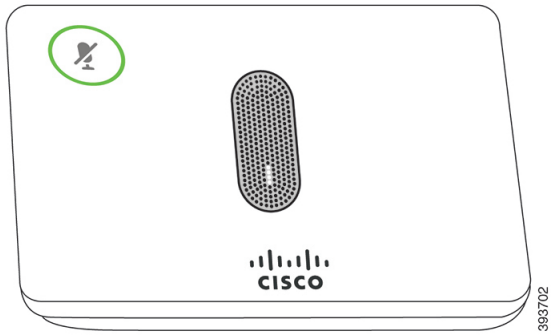
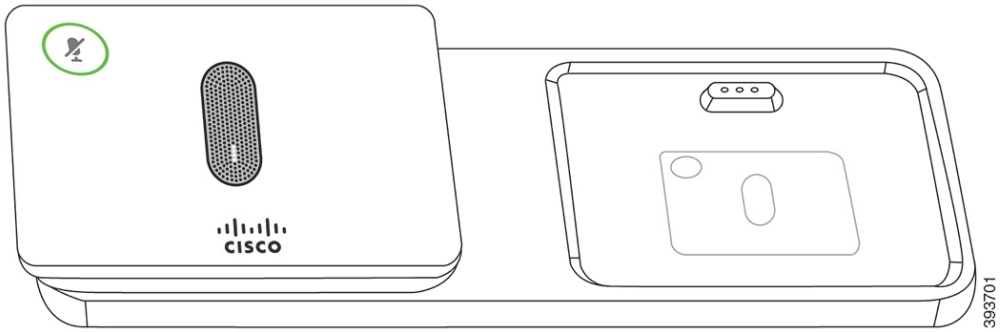


Figure 5: Wireless Microphone Mounted on the Charging Cradle



When the conference phone is in a call, the expansion microphone LED around the **Mute** button is lit green.

When the microphone is muted, the LED is lit red. When you press the **Mute** button, the phone and the expansion microphones are muted.

If the phone is paired with a wireless microphone (for example, Wireless microphone 1) and you connect the wireless microphone to a charger, pressing the **Show detail** softkey indicates the charge level for that microphone.

When the phone is paired with a wireless microphone and you connect a wired microphone, the wireless microphone gets unpaired and the phone is paired with the wired microphone. A notification appears on the phone screen indicating that the wired microphone is connected.

Related Topics

Install the Wireless Expansion Microphones, on page 36
Install the Wireless Microphone Charging Cradle, on page 37

Related Documentation

Use the following sections to obtain related information.

Cisco IP Conference Phone 8832 Documentation

Find documentation specific to your language, phone model, and call control system on the product support page for the Cisco IP Conference Phone 8832.

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 on the product support page.

Cisco Unified Communications Manager Express Documentation

See the publications that are specific to your language, phone model, and release on the product support page for Cisco Unified Communications Manager Express.

Cisco Hosted Collaboration Service Documentation

See the *Cisco Hosted Collaboration Solution Documentation Guide* and other publications that are specific to your Cisco Hosted Collaboration Solution release. Navigate from the following URL:

https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-hcs/tsd-products-support-series-home.html

Cisco Business Edition 4000 Documentation

See the *Cisco Business Edition 4000 Documentation Guide* and other publications that are specific to your Cisco Business Edition 4000 release. Navigate from the following URL:

https://www.cisco.com/c/en/us/support/unified-communications/business-edition-4000/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 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.

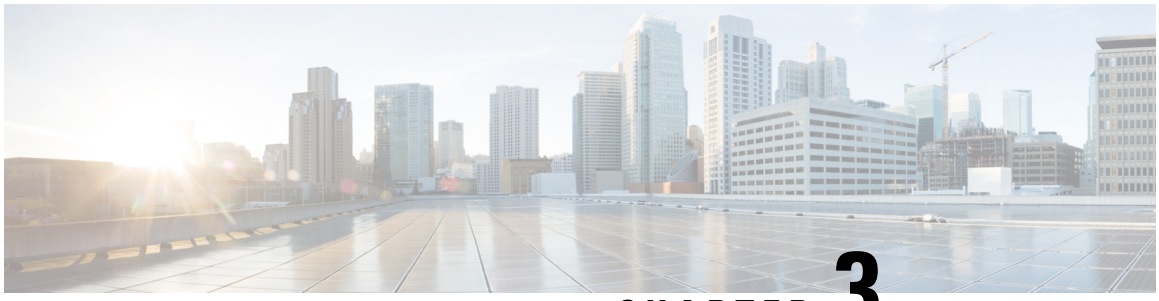
Terminology Differences

In this document, the term *Cisco IP Phone* includes the Cisco IP Conference Phone 8832.

The following table highlights some of the terminology differences in the *Cisco IP Conference Phone 8832 User Guide*, the *Cisco IP Conference Phone 8832 Administration Guide for Cisco Unified Communications Manager*, and the Cisco Unified Communications Manager documentation.

Table 6: Terminology Differences

User Guide	Administration Guide
Message Indicators	Message Waiting Indicator (MWI)
Voicemail System	Voice Messaging System



CHAPTER 3

Technical Details

Physical and Operating Environment Specifications

The following table shows the physical and operating environment specifications for the conference phone.

Table 7: Physical and Operating Specifications

Specification	Value or Range
Operating temperature	32° to 104°F (0° to 40°C)
Operating relative humidity	10% to 90% (noncondensing)
Storage temperature	14° to 140°F (–10° to 60°C)
Height	10.9 inches (278 mm)
Width	10.9 inches (278 mm)
Depth	2.4 inches (61.3 mm)
Weight	4.07 lb. (1852 g)
Power	IEEE PoE Class 3 via a PoE injector. The phone is compatible with Protocol and Link Layer Discovery Protocol - Power over Etherne Other options include a non-PoE Ethernet injector if the connected Phone 8832 Power Adapter is needed.

Specification	Value or Range
Security features	Secure boot
Cables	USB-C
Distance Requirements	The Ethernet Specification assumes that the maximum cable length be

For more information, see the *Cisco IP Conference Phone 8832 Data Sheet*: https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/datasheet-listing.html

Phone Power Requirements

The Cisco IP Conference Phone 8832 can use these power sources:

- Power over Ethernet (PoE) deployment with a Cisco IP Conference Phone 8832 PoE Injector
- Non-PoE Ethernet deployment with a Cisco IP Conference Phone 8832 Non-PoE Ethernet Injector
- Wi-Fi deployment with a Cisco IP Conference Phone 8832 Power Adapter

Table 8: Guidelines for Cisco IP Conference Phone Power

Power Type	Guidelines
PoE power—Provided by either the Cisco IP Conference Phone 8832 PoE Injector or Cisco IP Conference Phone 8832 Ethernet Injector through the USB-C cable attached to the phone.	If you are using either the Cisco IP Conference Phone 8832 PoE Injector or Cisco IP Conference Phone 8832 Ethernet Injector, make sure that the switch has a backup power supply to ensure uninterruptible operation of the phone. Ensure that the CatOS or IOS version that runs on your switch supports your intended phone deployment. See the documentation for your switch for operating system version information. When you install a phone that is powered by PoE, connect the injector to the LAN before you connect the USB-C cable to the phone. When you remove a phone that uses PoE, disconnect the USB-C cable from the phone before you remove the power from the adapter.

Power Type	Guidelines
External power • Non-PoE Ethernet deployment with a Cisco IP Conference Phone 8832 Non-PoE Ethernet Injector • Wi-Fi deployment with a Cisco IP Conference Phone 8832 Power Adapter • Non-PoE Ethernet deployment with a Cisco IP Conference Phone 8832 Ethernet Injector and a Cisco IP Conference Phone 8832 Power Adapter	When you install a phone that is powered with external power, connect the injector to power and to the Ethernet before you connect the USB-C cable to the phone. When you remove a phone that uses external power, disconnect the USB-C cable from the phone before you remove the power from the adapter.

Power Outage

Your access to emergency service through the phone requires that the phone receive power. If a power interruption occurs, service or emergency calling service dialing does not function until power is restored. If a power failure or disruption occurs, you may need to reset or reconfigure the equipment before you can use service or emergency calling service dialing.

Power Reduction

You can reduce the amount of energy that the Cisco IP Phone consumes by using Power Save or EnergyWise (Power Save Plus) mode.

Power Save

In Power Save mode, the backlight on the screen is not lit when the phone is not in use. The phone remains in Power Save mode for the scheduled duration or until the user presses any button.

Power Save Plus (EnergyWise)

The Cisco IP Phone supports Cisco EnergyWise (Power Save Plus) mode. When your network contains an EnergyWise (EW) controller (for example, a Cisco switch with the EnergyWise feature enabled), you can configure these phones to sleep (power down) and wake (power up) on a schedule to further reduce power consumption.

Set up each phone to enable or disable the EnergyWise settings. If EnergyWise is enabled, configure a sleep and wake time, as well as other parameters. These parameters are sent to the phone as part of the phone configuration XML file.

Related Topics

Schedule Power Save for Cisco IP Phone, on page 109
Schedule EnergyWise on Cisco IP Phone, on page 110

Network Protocols

The Cisco IP Conference Phone 8832 supports several industry-standard and Cisco network protocols that are required for voice communication. The following table provides an overview of the network protocols that the phones support.

Table 9: Supported Network Protocols on the Cisco IP Conference Phone

Network Protocol	Purpose	Usage Notes
Bootstrap Protocol (BootP)	BootP enables a network device, such as the phone, to discover certain startup information, such as its IP address.	—
Cisco Discovery Protocol (CDP)	CDP is a device-discovery protocol that runs on all Cisco-manufactured equipment. A device can use CDP to advertise its existence to other devices and receive information about other devices in the network.	The phone uses CDP to communicate information s of Service (QoS) configuration information with the
Dynamic Host Configuration Protocol (DHCP)	DHCP dynamically allocates and assigns an IP address to network devices. DHCP enables you to connect an IP phone into the network and have the phone 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 r on each phone locally. We recommend that you use DHCP custom option 1 value. For additional supported DHCP configuration Manager release. **Note** If you cannot use option 150, use DHC
Hypertext Transfer Protocol (HTTP)	HTTP is the standard protocol for transfer of information and movement of documents across the Internet and the web.	Phones use HTTP for XML services, provisioning,
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 suppo URL. A lock icon is displayed to the user if the connection
IEEE 802.1X	The IEEE 802.1X standard defines a client-server-based access control and authentication protocol that restricts unauthorized clients from connection 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 phone implements the IEEE 802.1X standard th EAP-TLS. When 802.1X authentication is enabled on the phon
Internet Protocol (IP)	IP is a messaging protocol that addresses and sends packets across the network.	To communicate with IP, network devices must hav IP addresses, subnets, and gateways identifications Configuration Protocol (DHCP). If you are not usin The phones support IPv6 address. For more informa Manager release.

Network Protocol	Purpose	Usage Notes
Link Layer Discovery Protocol (LLDP)	LLDP is a standardized network discovery protocol (similar to CDP) that is supported on some Cisco and third-party devices.	The phone supports LLDP on the PC port.
Link Layer Discovery Protocol-Media Endpoint Devices (LLDP-MED)	LLDP-MED is an extension of the LLDP standard developed for voice products.	The phone supports LLDP-MED on the SW por • Voice VLAN configuration • Device discovery • Power management • Inventory management For more information about LLDP-MED suppor https://www.cisco.com/en/US/tech/tk652/tk701/
Real-Time Transport Protocol (RTP)	RTP is a standard protocol for transporting real-time data, such as interactive voice and video, over data networks.	Phones use the RTP protocol to send and receive
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 de Unified Communications Manager or Media Gate on the endpoint itself.
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 is designed to add network. Signaling allows call information to be control the attributes of an end-to-end call.
Secure Real-Time Transfer protocol (SRTP)	SRTP is an extension of the Real-Time Protocol (RTP) Audio/Video Profile and ensures the integrity of RTP and Real-Time Control Protocol (RTCP) packets providing authentication, integrity, and encryption of media packets between two endpoints.	Phones use SRTP for media encryption.
Transmission Control Protocol (TCP)	TCP is a connection-oriented transport protocol.	Phones use TCP to connect to Cisco Unified Co
Transport Layer Security (TLS)	TLS is a standard protocol for securing and authenticating communications.	When security is implemented, phones use the T Manager. For more information, see the docume
Trivial File Transfer Protocol (TFTP)	TFTP allows you to transfer files over the network. On the phone, TFTP enables you to obtain a configuration file specific to the phone type.	TFTP requires a TFTP server in your network, v to use a TFTP server other than the one specified by using the Network Setup menu on the phone. For more information, see the documentation fo

Network Protocol	Purpose	Usage Notes
User Datagram Protocol (UDP)	UDP is a connectionless messaging protocol for delivery of data packets.	UDP is used only for RTP streams. SIP signaling or

Related Topics

Cisco Unified Communications Manager Documentation, on page 14

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 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 phones described in this chapter, see the documentation for your particular Cisco Unified Communications Manager release.

Note If the 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 device package for your version of Cisco Unified Communications Manager from Cisco.com.

Related Topics

Cisco Unified Communications Manager Documentation, on page 14

Cisco Unified Communications Manager Express Interaction

When your phone works with the Cisco Unified Communications Manager Express (Unified CME), it must go into CME mode.

When a user invokes the conference feature, the tag allows the phone to use either a local or network hardware conference bridge.

The phones do not support the following actions:

- Transfer—Only supported in the connected call transfer scenario.
- Conference—Only supported in the connected call transfer scenario.
- Join—Supported using the Conference button or hookflash access.

- Hold—Supported using the Hold button.
- Barge and Merge—Not supported.
- Direct Transfer—Not supported.
- Select—Not supported.

The users cannot create conference and transfer calls across different lines.

Unified CME supports intercom calls, also known as whisper paging. But the page is rejected by the phone during calls.

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.

  Make sure that you have used the Cisco Unified Communications Manager to configure the Messages button on the Cisco IP Phone.

- 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.

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

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.

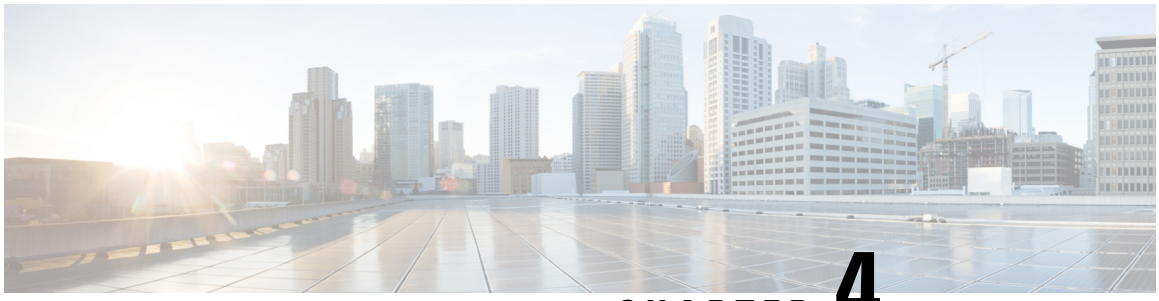
Application Programming Interface

Cisco supports phone API utilization by 3rd party applications that have been tested and certified through Cisco by the 3rd party application developer. Any phone issues related to uncertified application interaction must be addressed by the 3rd party and will not be addressed by Cisco.

For support model of Cisco certified 3rd party applications/solutions, please refer to Cisco Solution Partner Program website for details.

PART II

Cisco IP Conference Phone Installation



CHAPTER 4

Phone Installation

Verify the Network Setup

As they deploy a new IP telephony system, system administrators and network administrators must complete several initial configuration tasks to prepare the network for IP telephony service. For information and a checklist for setting up and configuring a Cisco IP telephony network, see the documentation for your particular Cisco Unified Communications Manager release.

For the phone to operate successfully as an endpoint in your network, your network must meet specific requirements. One requirement is the appropriate bandwidth. The phones require more bandwidth than the recommended 32 kbps when they register to Cisco Unified Communications Manager. Consider this higher bandwidth requirement when you configure your QoS bandwidth. For more information, refer to *Cisco Collaboration System 12.x Solution Reference Network Designs (SRND)* or later (https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab12/collab12.html).

Note The phone displays the date and time from Cisco Unified Communications Manager. The time displayed on the phone can differ from the Cisco Unified Communications Manager time by up to 10 seconds.

Procedure

Step 1 Configure a VoIP Network to meet the following requirements:

- VoIP is configured on your routers and gateways.
- Cisco Unified Communications Manager is installed in your network and is configured to handle call processing.

Step 2 Set up the network to support one of the following:

- DHCP support
- Manual assignment of IP address, gateway, and subnet mask

Related Topics

Cisco Unified Communications Manager Documentation, on page 14

Activation Code Onboarding for On-premises Phones

You can use Activation Code Onboarding to quickly set up new phones without autoregistration. With this approach, you control the phone onboarding process using the one of the following:

- Cisco Unified Communications Bulk Administration Tool (BAT)
- Cisco Unified Communications Manager Administration interface
- Administrative XML Web Service (AXL)

Enable this feature from the **Device Information** section of the Phone Configuration page. Select **Require Activation Code for Onboarding** if you want this feature to apply to a single on-premises phone.

Users must enter an activation code before their phones can register. Activation Code Onboarding can be applied to individual phones, a group of phones, or across an entire network.

This is an easy way for users to onboard their phones because they only enter a 16-digit activation code. Codes are entered either manually or with a QR code if a phone has a video camera. We recommend that you use a secure method to give users this information. But if a user is assigned to a phone, then this information is available on the Self Care Portal. The audit log records when a user accesses the code from the portal.

Activation codes can only be used once, and they expire after 1 week by default. If a code expires, you will have to provide the user with a new one.

You will find this approach an easy way to keep your network secure because a phone cannot register until the Manufacturing Installed Certificate (MIC) and activation code are verified. This method is also a convenient way to bulk onboard phones because it doesn't use the Tool for Auto-registered Phone Support (TAPS) or autoregistration. The rate of onboarding is one phone per second or about 3600 phones per hour. Phones can be added with the Cisco Unified Communications Manager Administrative, with Administrative XML Web Service (AXL), or with BAT.

Existing phones reset after they are configured for Activation Code Onboarding. They don't register until the activation code is entered and the phone MIC is verified. Inform current users that you are moving towards Activation Code Onboarding before you implement it.

For more information, see *Administration Guide for Cisco Unified Communications Manager and IM and Presence Service, Release 12.0(1)* or later.

Activation Code Onboarding and Mobile and Remote Access

You can use Activation Code Onboarding with Mobile and Remote Access when deploying Cisco IP phones for remote users. This feature is a secure way to deploy off-premises phones when autoregistration is not required. But you can configure a phone for autoregistration when on-premises, and activation codes when off-premises. This feature is similar to Activation Code Onboarding for on-premises phones, but it makes activation code available for off-premises phones also.

Activation Code Onboarding for Mobile and Remote Access requires Cisco Unified Communications Manager 12.5(1)SU1 or later, and Cisco Expressway X12.5 or later. Smart Licensing should be enabled also.

You enable this feature from the Cisco Unified Communications Manager Administration, but note the following:

- Enable this feature from the **Device Information** section of the Phone Configuration page.
- Select **Require Activation Code for Onboarding** if you want this feature to apply just to a single on-premises phone.
- Select **Allow Activation Code via MRA** and **Require Activation Code for Onboarding** if you want to use Activation Onboarding for a single off-premises phone. If the phone is on-premises, it changes to Mobile and Remote Access mode and uses the Expressway. If the phone cannot reach the Expressway, it does not register until it is off premises.

For more information, see the following documents:

- *Administration Guide for Cisco Unified Communications Manager and IM and Presence Service, Release 12.0(1)*
- *Mobile and Remote Access Through Cisco Expressway* for Cisco Expressway X12.5 or later

Enable Autoregistration for Phones

The Cisco IP Phone requires Cisco Unified Communications Manager to handle call processing. See the documentation for your particular Cisco Unified Communications Manager release or the context-sensitive help in the Cisco Unified Communications Manager Administration to ensure that Cisco Unified Communications Manager is set up properly to manage the phone and to properly route and process calls.

Before you install the Cisco IP Phone, you must choose a method for adding phones to the Cisco Unified Communications Manager database.

By enabling autoregistration before you install the phones, you can:

- Add phones without first gathering MAC addresses from the phones.
- Automatically add a Cisco IP Phone to the Cisco Unified Communications Manager database when you physically connect the phone to your IP telephony network. During autoregistration, Cisco Unified Communications Manager assigns the next available sequential directory number to the phone.
- Quickly enter phones into the Cisco Unified Communications Manager database and modify any settings, such as the directory numbers, from Cisco Unified Communications Manager.

- Move autoregistered phones to new locations and assign them to different device pools without affecting their directory numbers.

Autoregistration is disabled by default. In some cases, you might not want to use autoregistration; for example, if you want to assign a specific directory number to the phone, or if you want to use a secure connection with Cisco Unified Communications Manager. For information about enabling autoregistration, see the documentation for your particular Cisco Unified Communications Manager release. When you configure the cluster for mixed mode through the Cisco CTL client, autoregistration is automatically disabled, however you can enable it. When you configure the cluster for nonsecure mode through the Cisco CTL client, autoregistration is not enabled automatically.

You can add phones with autoregistration and TAPS, the Tool for AutoRegistered Phones Support, without first gathering MAC addresses from phones.

TAPS works with the Bulk Administration Tool (BAT) to update a batch of phones that were already added to the Cisco Unified Communications Manager database with dummy MAC addresses. Use TAPS to update MAC addresses and to download predefined configurations for phones.

Cisco recommends that you use autoregistration and TAPS to add fewer than 100 phones to your network. To add more than 100 phones to your network, use the Bulk Administration Tool (BAT).

To implement TAPS, you or the end user dials a TAPS directory number and follows voice prompts. After the process is complete, the phone contains the directory number and other settings, and the phone is updated in Cisco Unified Communications Manager Administration with the correct MAC address.

Verify that autoregistration is enabled and is properly configured in Cisco Unified Communications Manager Administration before you connect any Cisco IP Phone to the network. For information about enabling and configuring autoregistration, see the documentation for your particular Cisco Unified Communications Manager release.

Autoregistration must be enabled in Cisco Unified Communications Manager Administration for TAPS to function.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, click **System** > **Cisco Unified CM**.

Step 2 Click **Find** and select the required server.

Step 3 In **Auto-registration Information**, configure these fields.

- **Universal Device Template**
- **Universal Line Template**
- **Starting Directory Number**
- **Ending Directory Number**

Step 4 Uncheck the **Auto-registration Disabled on this Cisco Unified Communications Manager** check box.

Step 5 Click **Save**.

Step 6 Click **Apply Config**.

Daisy Chain Mode

You can connect two conference phones using a Smart Adapter and the USB-C cables that are provided in the daisy chain kit to expand the audio coverage area in a room.

In daisy chain mode, both units receive power though the Smart Adapter which is connected to a power adapter. You can use only one external microphone per unit. You can use either a pair of wired microphones with the units or a pair of wireless microphones with the units, but not a mixed combination of the microphones. When a wired microphone is connected to one of the units, it unpairs any wireless microphones that are connected to the same unit. Whenever there is an active call, the LEDs and the menu options on the phone screen of both units are synchronized.

Related Topics

Install the Conference Phone in Daisy Chain Mode, on page 38
One Phone in Daisy Chain Mode Doesn't Work, on page 163

Install the Conference Phone

After the phone connects to the network, the phone startup process begins, and the phone registers with Cisco Unified Communications Manager. If you disable the DHCP service, you must configure the network settings on the phone.

If you used autoregistration, you must update the specific configuration information for the phone such as associating the phone with a user, changing the button table, or directory number.

After the phone connects, it determines if a new firmware load has to be installed on the phone.

If you are using the conference phone in daisy chain mode, see Install the Conference Phone in Daisy Chain Mode, on page 38.

Before you begin

Ensure that you have the latest firmware version that is installed on your Cisco Unified Communications Manager. Check for updated device packages here:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/compat/matrix/CMDP_BK_CCBDA741_00_cucm-device-package-compatibility-matrix.html

Procedure

Step 1 Choose the power source for the phone:

- Power over Ethernet (PoE) deployment with a Cisco IP Conference Phone 8832 PoE Injector
- Non-PoE Ethernet deployment with a Cisco IP Conference Phone 8832 Non-PoE Ethernet Injector
- Wi-Fi deployment with a Cisco IP Conference Phone 8832 Power Adapter

For more information, see Ways to Provide Power to Your Conference Phone, on page 32.

Step 2 Connect the phone to the switch.

- If you use PoE:
  a. Plug the Ethernet cable into the LAN port.
  b. Plug the other end of the Ethernet cable into either the Cisco IP Conference Phone 8832 PoE Injector or the Cisco IP Conference Phone 8832 Ethernet Injector.
  c. Connect the injector to the conference phone with the USB-C cable.
- If you do not use PoE:
  a. If you are using the Cisco IP Conference Phone 8832 Ethernet Injector, plug the power adapter into an electrical outlet.
  b. Connect the power adapter to the Ethernet injector using a USB-C cable.

     OR

     If you are using the Cisco IP Conference Phone 8832 Non-PoE Ethernet Injector, plug it into an electrical outlet.
  c. Plug the Ethernet cable into the Non-PoE Ethernet injector or the Ethernet injector.
  d. Plug the Ethernet cable into the LAN port.
  e. Connect the Non-PoE Ethernet injector or the Ethernet injector to the conference phone using a USB-C cable.
- If you use Wi-Fi:
  a. Plug the Cisco IP Conference Phone 8832 Power Adapter into the electrical outlet.
  b. Connect the power adapter to the conference phone using a USB-C cable.

     Note Instead of the power adapter, you can use the Non-PoE Ethernet injector to get power to the phone. However, you must unplug the LAN cable. The phone only connects to Wi-Fi when the Ethernet connection is not available.

Step 3 Monitor the phone startup process. This step verifies that the phone is configured properly.

Step 4 If you do not use autoregistration, manually configure the security settings on the phone.

Step 5 Allow the phone to upgrade to the current firmware image that is stored on your Cisco Unified Communications Manager.

Step 6 Make calls with the phone to verify that the phone and features work correctly.

Step 7 Provide information to the users about how to use their phones and how to configure their phone options. This step ensures that users have adequate information to successfully use their Cisco phones.

Ways to Provide Power to Your Conference Phone

Your conference phone needs power from one of these sources:

- Power over Ethernet (PoE)
  - North America

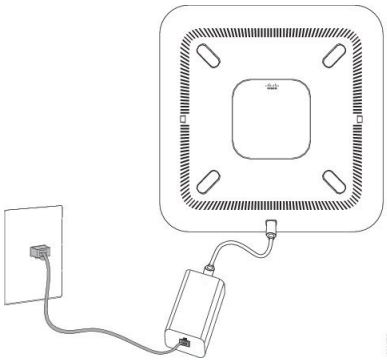
- Cisco IP Conference Phone 8832 PoE Injector
- Cisco IP Conference Phone 8832 Ethernet Injector

- Outside of North America—Cisco IP Conference Phone 8832 PoE Injector

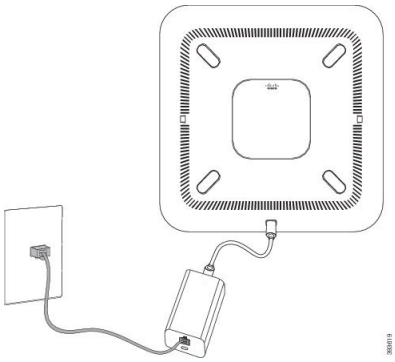
- Non-PoE Ethernet
  - North America
    - Cisco IP Conference Phone 8832 Non-PoE Ethernet Injector
    - Cisco IP Conference Phone 8832 Ethernet Injector with a Cisco IP Conference Phone 8832 Power Adapter connected to an electrical outlet.
  - Outside of North America—Cisco IP Conference Phone 8832 Non-PoE Ethernet Injector
- WiFi—Use the Cisco IP Conference Phone 8832 Power Adapter connected to an electrical outlet.

Figure 6: Conference Phone PoE Power Options

The following figure shows the two PoE power options.



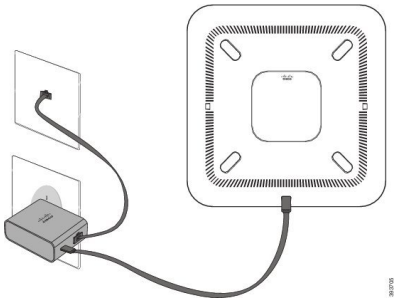
Cisco IP Conference Phone 8832 PoE Injector with the PoE power option



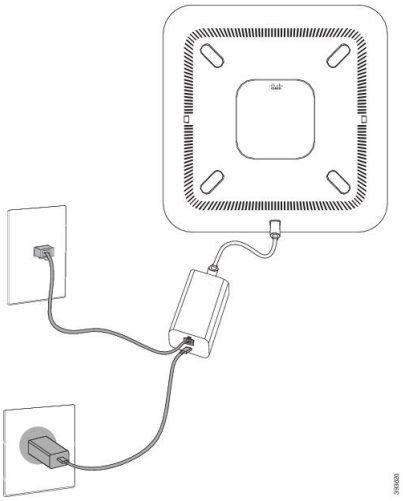
Cisco IP Conference Phone 8832 Ethernet Injector with the PoE power option

Figure 7: Conference Phone Ethernet Power Options

The following figure shows the two Ethernet power options.



Cisco IP Conference Phone 8832 Non-PoE Ethernet Injector with the Ethernet power option



Cisco IP Conference Phone 8832 Ethernet Injector with the Ethernet power option

Figure 8: Conference Phone Power Option When Connected to a Wi-Fi Network

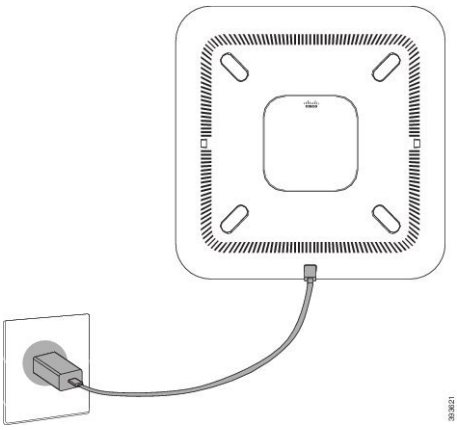
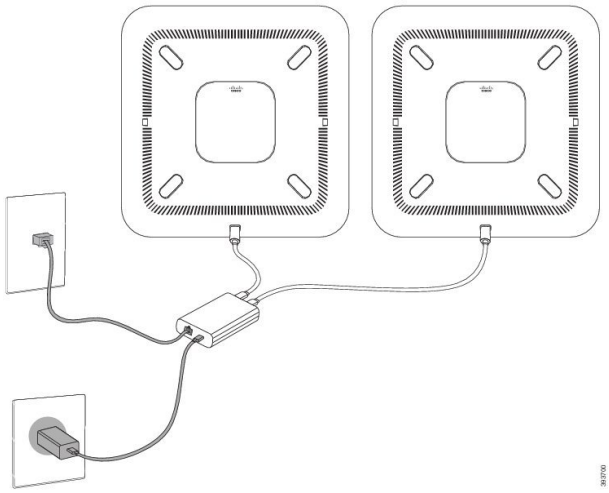


Figure 9: Conference Phone Power Option in Daisy Chain Mode

The following figure shows the power option when the phone is connected in daisy chain mode.



Install the Wired Expansion Microphones

The phone supports an optional kit with two wired expansion microphones. You can extend the microphones up to 7 feet (2.13m) from the phone. For best results, place the microphones between 3 feet (0.91 m) and 7 feet (2.1 m) away from the phone.

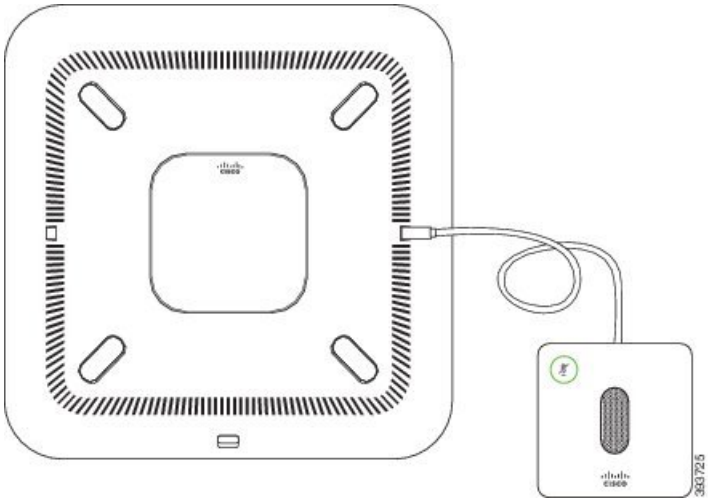
Procedure

Step 1 Plug the end of the microphone cable into the port on the side of the phone.

Step 2 Extend the microphone cable to the desired position.

The following figure shows installation of a wired expansion microphone.

Figure 10: Wired Expansion Microphone Installation



Install the Wireless Expansion Microphones

The conference phone provides the option of connecting two wireless expansion microphones.

Note You must use either two wired microphones or two wireless microphones with the phone, but not a mixed combination.

When the phone is in a call, the LED on the expansion microphone is lit green. To mute the expansion microphone, press the **Mute** key. When the microphone is muted, the LED is lit red. When the battery in the microphone is low, the battery indication LED blinks rapidly.

Before you begin

Disconnect the wired expansion microphones before you install wireless expansion microphones. You cannot use both wired and wireless expansion microphones at the same time.

Procedure

Step 1 Position the table mount plate on the table surface location where you want to place the microphone.

Step 2 Remove the adhesive for the double-stick tape on the bottom of the table mount plate. Place the table mount plate to adhere to the table surface.

Step 3 Attach the microphone to the table mount plate. Magnets are embedded in the microphone to snap the unit into place.

You can move the microphone and attached table mount to a different location on the table surface as needed. Use care when moving to protect the unit.

Related Topics

Wireless Expansion Microphone (8832 Only), on page 13
Install the Wireless Microphone Charging Cradle, on page 37

Install the Wireless Microphone Charging Cradle

You use the charging cradle to charge the wireless microphone battery.

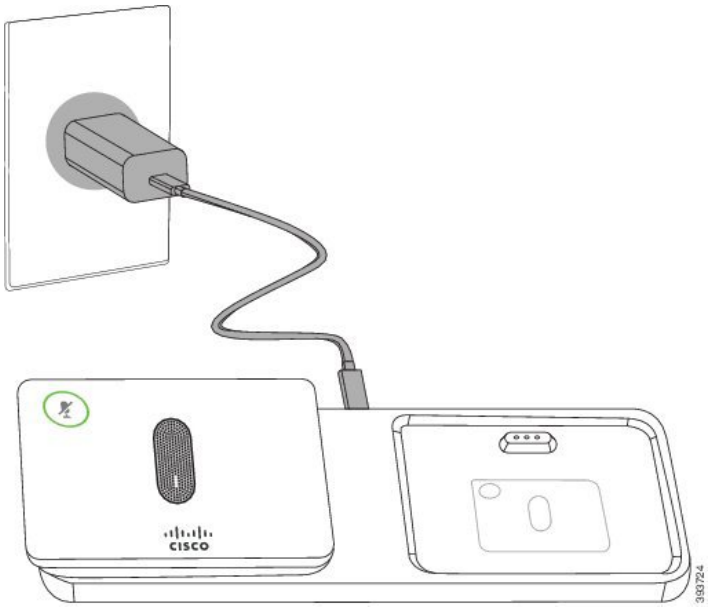
Procedure

Step 1 Plug the charging cradle power adapter into an electrical outlet.

Step 2 Plug one end of the USB-C cable to the charging cradle and the other end into the power adapter.

The following figure shows installation of a wireless microphone charging cradle.

Figure 11: Wireless Microphone Charging Cradle Installation



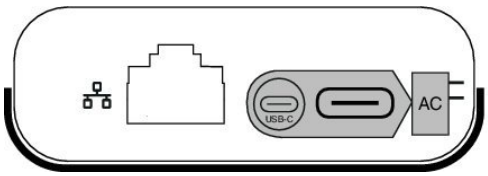
Related Topics

Wireless Expansion Microphone (8832 Only), on page 13
Install the Wireless Expansion Microphones, on page 36

Install the Conference Phone in Daisy Chain Mode

The daisy chain kit contains a Smart Adapter, a short LAN cable, two long, thicker USB-C cables, and a shorter, thinner USB-C cable. In daisy chain mode, the conference phones require external power from an electrical outlet. You must use the Smart Adapter to connect the phones together. The long USB-C cables go to the phone and the short one goes to the power adapter. Refer to the following figure when you connect the power adapter and the LAN port to the Smart Adapter.

Figure 12: Smart Adapter Power Port and LAN Port



You can use only one microphone per unit.

Note You must use either two wired microphones or two wireless microphones with the phone, but not a mixed combination.

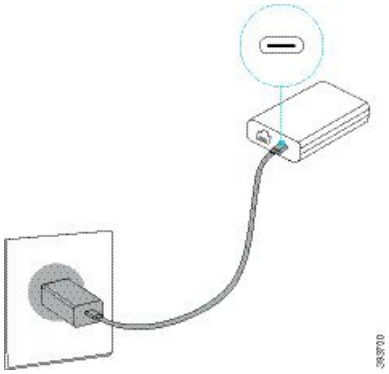
The USB-C cable for the power adapter is thinner than the USB-C cables that connect to the phone.

Procedure

Step 1 Plug the power adapter into the electrical outlet.

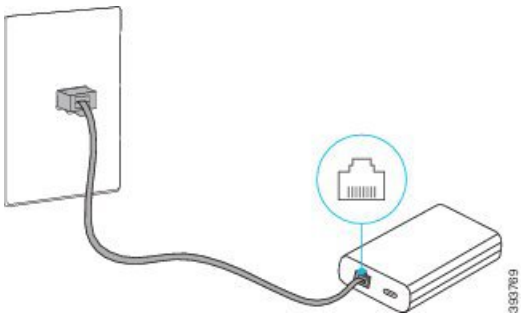
Step 2 Connect the short, thinner USB-C cable from the power adapter to the Smart Adapter.

Figure 13: Smart Adapter USB Port Connected to the Power Outlet



Step 3 Required: Connect the Ethernet cable to the Smart Adapter and the LAN port.

Figure 14: Smart Adapter LAN Port Connected to the LAN Port on the Wall Outlet

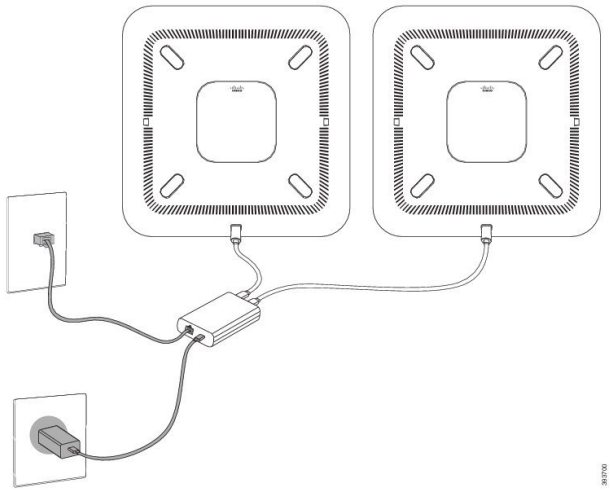


Step 4 Connect the first phone to the Smart Adapter using the longer, thicker USB-C cable.

Step 5 Connect the second phone to the Smart Adapter using a USB-C cable.

The following figure shows installation of the conference phone in daisy chain mode.

Figure 15: Conference Phone Installation in Daisy Chain Mode



Related Topics

Daisy Chain Mode, on page 31
One Phone in Daisy Chain Mode Doesn't Work, on page 163

Reboot Your Conference Phone from the Backup Image

Your Cisco IP Conference Phone 8832 has a second, backup image that allows you to recover the phone when the default image has been compromised.

To reboot your phone from the backup image, perform the following procedure.

Procedure

Step 1 Hold the * key while connecting the power to the conference phone.

Step 2 After the LED bar light turns ON green and then OFF, you can release the * key.

Step 3 The conference phone reboots from the backup image.

Set Up the Phone from the Setup Menus

The phone includes many configurable network settings that you may need to modify before the phone is functional for your users. You can access these settings, and change some of them, through menus on the phone.

The phone includes the following setup menus:

- Network Setup: Provides options for viewing and configuring a variety of network settings.
  - IPv4 Setup: This submenu provides additional network options.
  - IPv6 Setup: This submenu provides additional network options.
- Security Setup: Provides options for viewing and configuring a variety of security settings.

Note You can control whether a phone has access to the Settings menu or to options on this menu. Use the **Settings Access** field in the Cisco Unified Communications Manager Administration Phone Configuration window to control access. The **Settings Access** field accepts these values:

- Enabled: Allows access to the Settings menu.
- Disabled: Prevents access to most entries in the Settings menu. The user can still access **Settings** > **Status**.
- Restricted: Allows access to the User Preferences and Status menu items and allows volume changes to be saved. Prevents access to other options on the Settings menu.

If you cannot access an option on the Admin Settings menu, check the **Settings Access** field.

You configure settings that are display-only on the phone in Cisco Unified Communications Manager Administration.

Procedure

Step 1 Press **Settings**.

Step 2 Select **Admin Settings**.

Step 3 Enter password if required, then click **Sign-In**.

Step 4 Select **Network Setup** or **Security Setup**.

Step 5 Perform one of these actions to display the desired menu:

- Use the navigation arrows to select the desired menu and then press **Select**.
- Use the keypad on the phone to enter the number that corresponds to the menu.

Step 6 To display a submenu, repeat step 5.

Step 7 To exit a menu, press **Back**.

Related Topics

Restart or Reset the Conference Phone, on page 171
Configure the Network Settings, on page 42
Configure the Security Settings

Apply a Phone Password

Procedure

Step 1 In Cisco Unified Communications Manager Administration, navigate to the Common Phone Profile Configuration window (**Device** > **Device Settings** > **Common Phone Profile**).

Step 2 Enter a password in the Local Phone Unlock Password option.

Step 3 Apply the password to the common phone profile that the phone uses.

Text and Menu Entry From the Phone

When you edit the value of an option setting, follow these guidelines:

- Use the arrows on the navigation pad to highlight the field that you wish to edit. Press **Select** in the navigation pad to activate the field. After the field is activated, you can enter values.
- Use the keys on the keypad to enter numbers and letters.
- To enter letters by using the keypad, use a corresponding number key. Press the key one or more times to display a particular letter. For example, press the **2** key once for "a," twice quickly for "b," and three times quickly for "c." After you pause, the cursor automatically advances to allow you to enter the next letter.
- Press the softkey ⌫ if you make a mistake. This softkey deletes the character to the left of the cursor.
- Press **Revert** before pressing **Apply** to discard any changes that you made.
- To enter a period (for example, in an IP address), press ***** on the keypad.
- To enter a colon for an IPv6 address, press ***** on the keypad.

Note The Cisco IP Phone provides several methods to reset or restore option settings, if necessary.

Configure the Network Settings

Procedure

Step 1 Press **Settings**.

Step 2 Select **Admin Settings** > **Network Setup** > **Ethernet setup**.

Step 3 Set the fields as described in Network Setup Fields, on page 42.
After you set the fields, you may need to reboot the phone.

Network Setup Fields

The Network Setup menu contains fields and submenus for IPv4 and IPv6.

To change some of the fields, you need to turn DHCP off.

Table 10: Network Setup Menu

Entry	Type	Default	Description
IPv4 setup	Menu		See the “IPv4 Setup Submenu” table. This option displays only when the mode or in dual-stack mode.
IPv6 setup	Menu		See the “IPv6 Setup Submenu” table.
Host name	String		Host name of the phone. If using DHCP, this name is automatically assigned.
Domain name	String		Name of the Domain Name System (DNS) domain in which the phone resides. To change this field, turn off DHCP.
Operational VLAN ID			Operational Virtual Local Area Network (VLAN) that is configured on a Cisco Catalyst switch in which the phone is a member.
Admin VLAN ID			Auxiliary VLAN in which the phone is a member.

Entry	Type	Default	Description
SW Port Setup	Auto Negotiate 10 Half 10 Full 100 Half 100 Full	Auto Negotiate	Speed and duplex of the switch port, where: • 10 Half = 10-BaseT/half duplex • 10 Full = 10-BaseT/full duplex • 100 Half = 100-BaseT/half duplex • 100 Full = 100-BaseT/full duplex
LLDP-MED: SW Port	Disabled Enabled	Enabled	Indicates whether Link Layer Discovery Protocol Media Endpoint Discovery (LLDP-MED) is enabled on the switch port.

Table 11: IPv4 Setup Submenu

Entry	Type	Default	Description
DHCP	Disabled Enabled	Enabled	Enables or disables the use of DHCP.
IP Address			Internet Protocol version 4 (IPv4) address of the phone. To change this field, turn off DHCP.
Subnet Mask			Subnet mask that the phone uses. To change this field, turn off DHCP.
Default Router 1			Default router used that the phone uses. To change this field, turn off DHCP.
DNS Server 1			Primary Domain Name System (DNS) server (DNS Server 1) that the phone uses. To change this field, turn off DHCP.
DNS Server 2			Primary Domain Name System (DNS) server (DNS Server 2) that the phone uses.
DNS Server 3			Primary Domain Name System (DNS) server (DNS Server 3) that the phone uses.
Alternate TFTP	No Yes	No	Indicates whether the phone is using an alternative TFTP server.

Entry	Type	Default	Description
TFTP Server 1			Primary Trivial File Transfer Protocol (TFTP) server that the phone uses. If you set the Alternate TFTP option to On, you must enter a nonzero value for the TFTP Server 1 option. If neither the primary TFTP server nor the backup TFTP server is listed in the CTL or ITL file on the phone, you must unlock the file before you can save changes to the TFTP Server 1 option. In this case, the phone deletes the file when you save changes to the TFTP Server 1 option. A new CTL or ITL file downloads from the new TFTP Server 1 address. See the TFTP notes after the final table.
TFTP Server 2			Secondary TFTP server that the phone uses. If neither the primary TFTP server nor the backup TFTP server is listed in the CTL or ITL file on the phone, you must unlock the file before you can save changes to the TFTP Server 2 option. In this case, the phone deletes the file when you save changes to the TFTP Server 2 option. A new CTL or ITL file downloads from the new TFTP Server 2 address. See the TFTP Notes section after the final table.
DHCP Address Released	No Yes	No	

Table 12: IPv6 Setup Submenu

Entry	Type	Default	Description
DHCPv6 Enabled	Disabled Enabled	Enabled	Enables or disables the use of IPv6 DHCP.
IPv6 Address			The IPv6 address of the phone. To change this field, turn off DHCP.
IPv6 Prefix Length			Length of the IPv6 address. To change this field, turn off DHCP.

Entry	Type	Default	Description
IPv6 Default Router 1			Default IPv6 router. To change this field, turn off DHCP.
IPv6 DNS Server 1			Primary IPv6 DNS server To change this field, turn off DHCP.
IPv6 Alternate TFTP	No Yes	No	Indicates whether the phone is using an alternative IPv6 TFTP server.
IPv6 TFTP Server 1			Primary IPv6 TFTP server used that the phone uses. See the TFTP Notes section after this table.
IPv6 TFTP Server 2			Secondary IPv6 TFTP server used that the phone uses. See the TFTP Notes section after this table.
IPv6 Address Released	No Yes	No	

Before IPv6 setup options can be configured on your device, IPv6 must be enabled and configured in Cisco Unified Communication Administration. The following device configuration fields apply to IPv6 configuration:

- IP Addressing Mode
- IP Addressing Mode Preference for Signalling

If IPv6 is enabled in the Unified cluster, the default setting for IP addressing mode is IPv4 and IPv6. In this addressing mode, the phone will acquire and use one IPv4 address and one IPv6 address. It can use the IPv4 and the IPv6 address as required for media. The phone uses either the IPv4 or IPv6 address for call control signalling.

For more information about IPv6, see:

- "Common Device Configuration" in *Cisco Unified Communications Manager Feature and Services Guide*, "IPv6 Support in Cisco Unified Communications Devices" chapter.
- *IPv6 Deployment Guide for Cisco Collaboration Systems Release 12.0*, located here: https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-system/products-implementation-design-guides-list.html

TFTP Notes

When the phone looks for the TFTP server, the phone gives precedence to manually assigned TFTP servers, regardless of the protocol. If your configuration includes both IPv6 and IPv4 TFTP servers, the phone prioritizes the order that it looks for the TFTP server by giving priority to manually assigned IPv6 TFTP servers and IPv4 TFTP servers. The phone looks for the TFTP server in this order:

1. Any manually assigned IPv4 TFTP servers
2. Any manually assigned IPv6 servers
3. DHCP assigned TFTP servers
4. DHCPv6 assigned TFTP servers

For information about the CTL and ITL files, see the *Cisco Unified Communications Manager Security Guide*.

Set Domain Name Field

Procedure

Step 1 Set the DHCP Enabled option to **No**.
Step 2 Scroll to the Domain Name option, press **Select**, and enter a new domain name.
Step 3 Press **Apply**.

Enable Wireless LAN from the Phone

Ensure that the Wi-Fi coverage in the location where the wireless LAN is deployed is suitable for transmitting voice packets.

A fast-secure roaming method is recommended for Wi-Fi users. We recommend that you use 802.11r (FT).

For complete configuration information, see the *Cisco IP Phone 8832 Wireless LAN 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

The *Cisco IP Phone 8832 Wireless LAN Deployment Guide* includes the following configuration information:

- Wireless network configuration
- Wireless network configuration in Cisco Unified Communications Manager Administration
- Wireless network configuration on the Cisco IP Phone

Before you begin

Make sure that Wi-Fi is enabled on the phone, and the Ethernet cable is disconnected.

Procedure

Step 1 To enable the application, press **Settings**.
Step 2 Navigate to **Admin settings** > **Network setup** > **Wi-Fi client setup** > **Wireless**.

Step 3 Press **On**.

Set Up the Wireless LAN from Cisco Unified Communications Manager

In Cisco Unified Communications Manager Administration, you must enable a parameter called "Wi-Fi" for the conference phone.

Note In the Phone Configuration window in Cisco Unified Communications Manager Administration (**Device** > **Phone**), use the wired-line MAC address when you configure the MAC address. Cisco Unified Communications Manager registration does not use the wireless MAC address.

Perform the following procedure in Cisco Unified Communications Manager Administration.

Procedure

Step 1 To enable the wireless LAN on a specific phone, perform the following steps:

a) Select **Device** > **Phone**.
b) Locate the required phone.
c) Select the **Enabled** setting for the Wi-Fi parameter in the Product Specific Configuration Layout section.
d) Check the **Override Common Settings** check box.

Step 2 To enable wireless LAN for a group of phones,

a) Select **Device** > **Device Settings** > **Common Phone Profile**.
b) Select the **Enabled** setting for the Wi-Fi parameter.

Note To ensure that the configuration in this step works, uncheck the **Override Common Settings** check box mentioned in Step 1d.

c) Check the **Override Common Settings** check box.
d) Associate the phones with that common phone profile using **Device** > **Phone**.

Step 3 To enable wireless LAN for all WLAN-capable phones in your network,

a) Select **System** > **Enterprise Phone Configuration**.
b) Select the **Enabled** setting for the Wi-Fi parameter.

Note To ensure that the configuration in this step works, uncheck the **Override Common Settings** check box mentioned in Step 1d and Step 2c.

c) Check the **Override Common Settings** check box.

Set Up Wireless LAN from the Phone

Before the Cisco IP Phone can connect to the WLAN, you must configure the network profile for the phone with the appropriate WLAN settings. You can use the **Network setup** menu on the phone to access the **Wi-Fi client setup** submenu and set up the WLAN configuration.

Note The **Wi-Fi client setup** option does not appear in the **Network setup** menu when Wi-Fi is disabled on the Cisco Unified Communications Manager.

For additional information, see *Cisco IP Conference Phone 8832 WLAN Deployment Guide*, located here: http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-implementation-design-guides-list.html

Before you begin

Configure the wireless LAN from Cisco Unified Communications Manager.

Procedure

Step 1 Press **Settings**.

Step 2 Select **Admin settings** > **Network setup** > **Wi-Fi client setup**.

Step 3 Set up the wireless configuration as described in the following table.

Table 13: Wi-Fi Client Setup Menu Options

Option	Description	To change
Wireless	Turns the wireless radio on the Cisco IP Phone on or off.	Scroll to the **Wireless** option, and use switch to change the setting between C
Network name	Enables you to connect to a wireless network using the **Choose a Network** window. This window has two softkeys - **Back** and **Other**.	In the **Choose a Network** window, se network that you wish to connect to.
Wi-Fi sign in access	Enables the display of the Wi-Fi sign in window.	Scroll to **Wi-Fi sign in access** option, the toggle switch to change the setting On and Off.
IPv4 setup	In the IPv4 Setup configuration submenu, you can do the following: • Enable or disable the phone to use the IP address that the DHCP server assigns. • Manually set the IP Address, Subnet Mask, Default Routers, DNS Server, and Alternate TFTP servers. For more information about the IPv4 address fields, see the “IPv4 Setup Submenu” table.	Scroll to **IPv4 setup** and press **Select**.

Option	Description	To change
IPv6 setup	In the IPv6 setup configuration submenu, you can do the following: • Enable or disable the phone to use the IPv6 address that is either assigned by DHCPv6 server or acquired by SLAAC through an IPv6-enabled router. • Manually set the IPv6 Address, Prefix Length, Default Routers, DNS Server, and Alternate TFTP servers. For more information about the IPv6 address fields, see the "IPv6 Setup Submenu" table.	Scroll to **IPv6 setup** and press **Sel**
MAC address	Unique Media Access Control (MAC) address of the phone.	Display only. Cannot configure.
Domain name	Name of the Domain Name System (DNS) domain in which the phone resides.	See Set Domain Name Field, on p

Step 4 Press **Save** to make changes or press **Revert** to discard the connection.

Set the Number of WLAN Authentication Attempts

An authentication request is a confirmation of the user's sign-in credentials. It occurs whenever a phone that has already joined a Wi-Fi network tries to reconnect to the Wi-Fi server. Examples include when a Wi-Fi session times out or a Wi-Fi connection is lost and then reacquired.

You can configure the number of times a Wi-Fi phone sends an authentication request to the Wi-Fi server. The default number of attempts is 2, but you can set this parameter from 1 to 3. If a phone fails the authentication, then the user is prompted to sign in again.

You can apply WLAN Authentication Attempts to individual phones, to a pool of phones, or to all the Wi-Fi phones in your network.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, select **Device** > **Phone** and locate the phone.
Step 2 Navigate to the Product Specific Configuration area and set the **WLAN Authentication Attempts** field.
Step 3 Select **Save**.
Step 4 Select **Apply Config**.
Step 5 Restart the phone.

Enable WLAN Prompt Mode

Enable WLAN Profile 1 Prompt Mode if you want a user to sign into the Wi-Fi network when their phone powers-up or resets.

Procedure

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

Step 2 Locate the phone that you need to set up.

Step 3 Navigate to the Product Specific Configuration area and set the **WLAN Profile 1 Prompt Mode** field to **Enable**.

Step 4 Select **Save**.

Step 5 Select **Apply Config**.

Step 6 Restart the phone.

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 only support one server certificate which can be installed either with SCEP or the manual install method but not both methods. The phones don't support the TFTP method of certificate installation.

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.

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.

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.

When more that one wireless LAN profile is selected, the phone uses only the first wireless LAN profile.

Step 5 Click **Save**.

Verify the Phone Startup

After the phone has power connected to it, it automatically cycles through a startup diagnostic process.

Procedure

Power up the phone.

When the main screen displays, it has started up properly.

Change a User's Phone Model

You or your user can change a user's phone model. The change can be required for a number of reasons, for example:

- You have updated your Cisco Unified Communications Manager (Unified CM) to a software version that doesn't support the phone model.
- The user wants a different phone model from their current model.
- The phone requires repair or replacement.

The Unified CM identifies the old phone and uses the old phone's MAC address to identify the old phone configuration. The Unified CM copies the old phone configuration into the entry for the new phone. The new phone then has the same configuration as the old phone.

Limitation: If the old phone has more lines or line buttons than the new phone, the new phone doesn't have the extra lines or line buttons configured.

The phone reboots when the configuration is complete.

Before you begin

Set up your Cisco Unified Communications Manager according to the instructions in the *Feature Configuration Guide for Cisco Unified Communications Manager*.

You need a new, unused phone that comes preinstalled with Firmware Release 12.8(1) or later.

Procedure

Step 1 Power off the old phone.

Step 2 Power on the new phone.

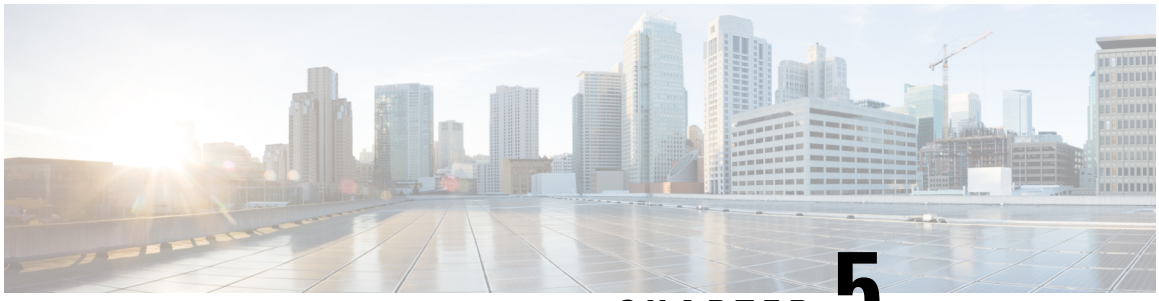
Step 3 On the new phone, select **Replace an existing phone**.

Step 4 Enter the primary extension of the old phone.

Step 5 If the old phone had a PIN assigned, enter the PIN.

Step 6 Press **Submit**.

Step 7 If there is more than one device for the user, select the device to replace and press **Continue**.



CHAPTER 5

Cisco Unified Communications Manager Phone Installation

Set up a Cisco IP Conference Phone

If autoregistration is not enabled and the phone does not exist in the Cisco Unified Communications Manager database, you must manually configure the Cisco IP Phone in Cisco Unified Communications Manager Administration. Some tasks in this procedure are optional, depending on your system and user needs.

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

Perform the configuration steps in the following procedure using Cisco Unified Communications Manager Administration.

Procedure

Step 1 Gather the following information about the phone:

- Phone model
- MAC address: see Determine the Phone MAC Address, on page 59
- Physical location of the phone
- Name or user ID of phone user
- Device pool
- Partition, calling search space, and location information

- Directory number (DN) to assign to the phone
- Cisco Unified Communications Manager user to associate with the phone
- Phone usage information that affects the softkey template, phone features, IP Phone services, or phone applications

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

Step 2 Verify that you have sufficient unit licenses for your phone.

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

Step 3 Define the Device Pools. Select **System** > **Device Pool**.

Device Pools define common characteristics for devices, such as region, date/time group, and softkey template.

Step 4 Define the Common Phone Profile. Select **Device** > **Device settings** > **Common Phone Profile**.

Common phone profiles provide data that the Cisco TFTP server requires, as well as common phone settings, such as Do Not Disturb and feature control options.

Step 5 Define a Calling Search Space. In Cisco Unified Communications Manager Administration, click **Call Routing** > **Class of Control** > **Calling Search Space**.

A Calling Search Space is a collection of partitions that are searched to determine how a dialed number is routed. The calling search space for the device and the calling search space for the directory number are used together. The directory number CSS takes precedence over the device CSS.

Step 6 Configure a security profile for the device type and protocol. Select **System** > **Security** > **Phone Security Profile**.

Step 7 Set up the phone. Select **Device** > **Phone**.

a) Locate the phone you want to modify, or add a new phone.
b) Configure the phone by completing the required fields in the Device Information pane of the Phone Configuration window.
   - MAC Address (required): Make sure that the value comprises 12 hexadecimal characters.
   - Description: Enter a useful description to help you if you need to search on information about this user.
   - Device Pool (required)
   - Common Phone Profile
   - Calling Search Space
   - Location
   - Owner (User or Anonymous), and if User is selected, the Owner User ID

   The device with its default settings is added to the Cisco Unified Communications Manager database.

   For information about Product Specific Configuration fields, see the "?" Button Help in the Phone Configuration window and the related link.

Note If you want to add both the phone and user to the Cisco Unified Communications Manager database at the same time, see the documentation for your particular Cisco Unified Communications Manager release.

c) In the Protocol Specific Information area of this window, choose a Device Security Profile and set the security mode.

Note Choose a security profile based on the overall security strategy of the company. If the phone does not support security, choose a nonsecure profile.

d) In the Extension Information area, check the Enable Extension Mobility check box if this phone supports Cisco Extension Mobility.

e) Click **Save**.

Step 8 Select **Device** > **Device Settings** > **SIP Profile** to set up SIP parameters.

Step 9 Select **Device** > **Phone** to configure directory numbers (lines) on the phone by completing the required fields in the Directory Number Configuration window.

a) Find the phone.

b) In the Phone Configuration window, click Line 1 on the left pane of the window.

Conference phones have only one line.

c) In the Directory Number field, enter a valid number that can be dialed.

Note This field should contain the same number that appears in the Telephone Number field in the End User Configuration window.

d) From the Route Partition drop-down list, choose the partition to which the directory number belongs. If you do not want to restrict access to the directory number, choose <None> for the partition.

e) From the Calling Search Space drop-down list, choose the appropriate calling search space. The value that you choose applies to all devices that are using this directory number.

f) In the Call Forward and Call Pickup Settings area, choose the items (for example, Forward All, Forward Busy Internal) and corresponding destinations to which calls should be sent.

Example:

If you want incoming internal and external calls that receive a busy signal to forward to the voice mail for this line, check the Voice Mail check box next to the Forward Busy Internal and Forward Busy External items in the left column of the Call Pickup and Call Forward Settings area.

g) In the Line 1 on Device pane, configure the following fields:

- Display (Internal Caller ID field): You can enter the first name and last name of the user of this device so that this name displays for all internal calls. Leave this field blank to have the system display the phone extension.
- External Phone Number Mask: Indicate phone number (or mask) that is used to send Caller ID information when a call is placed from this line. You can enter a maximum of 24 numeric and "X" characters. The Xs represent the directory number and must appear at the end of the pattern.

Example:

If you specify a mask of 408902XXXX, an external call from extension 6640 displays a caller ID number of 4089026640.

This setting applies only to the current device unless you check the check box at the right (Update Shared Device Settings) and click **Propagate Selected**. The check box at the right displays only if other devices share this directory number.

h) Select **Save**.

For more information about directory numbers, see the documentation for your particular Cisco Unified Communications Manager release and the related links.

Step 10 (Optional) Associate the user with a phone. Click **Associate End Users** at the bottom of the Phone Configuration window to associate a user to the line that is being configured.

a) Use **Find** in conjunction with the Search fields to locate the user.
b) check the box next to the user name, and click **Add Selected**.

The user name and user ID appears in the Users Associated With Line pane of the Directory Number Configuration window.

c) Select **Save**.

The user is now associated with Line 1 on the phone.

Step 11 (Optional) Associate the user with the device:

a) Choose **User Management** > **End User**.
b) Use the search boxes and **Find** to locate the user you have added.
c) Click on the user ID.
d) In the Directory Number Associations area of the screen, set the Primary Extension from the drop-down list.
e) (Optional) In the Mobility Information area, check the Enable Mobility box.
f) In the Permissions Information area, use the **Add to Access Control Group** buttons to add this user to any user groups.

For example, you may want to add the user to a group that is defined as a Standard CCM End User Group.

g) To view the details of a group, select the group and click **View Details**.
h) In the Extension Mobility area, check the Enable Extension Mobility Cross Cluster box if the user can use for Extension Mobility Cross Cluster service.
i) In the Device Information area, click **Device Associations**.
j) Use the Search fields and **Find** to locate the device that you want to associate to the user.
k) Select the device, and click **Save Selected/Changes**.
l) Click **Go** next to the “Back to User” Related link in the upper right corner of the screen.
m) Select **Save**.

Step 12 Customize the softkey templates. Select **Device** > **Device Settings** > **Softkey Template**.

Use the page to add, delete, or change the order of softkey features that display on the user’s phone to meet feature usage needs.

The conference phone has special softkey requirements. See the related links for more information.

Step 13 Configure Cisco IPPhone services and assign services. Select **Device** > **Device Settings** > **Phone Services**.

Provides IP Phone services to the phone.

Note Users can add or change services on their phones using the Cisco Unified Communications Self Care Portal.

Step 14 (Optional) Add user information to the global directory for Cisco UnifiedCommunications Manager. Select **User Management** > **End User**, and then click **Add New** and configure the required fields. Required fields are indicated by an asterisk (*).

Note If your company uses a Lightweight Directory Access Protocol (LDAP) directory to store information on users, you can install and configure Cisco Unified Communications to use your existing LDAP directory, see Corporate Directory Setup, on page 123. After the Enable Synchronization from the LDAP Server field is enabled, you will not be able to add additional users from Cisco Unified Communications Manager Administration.

a) Set the User ID and last name fields.
b) Assign a password (for Self Care Portal).
c) Assign a PIN (for Cisco Extension Mobility and Personal Directory).
d) Associate the user with a phone.

Provides users with control over their phone such as forwarding calls or adding speed-dial numbers or services.

Note Some phones, such as those in conference rooms, do not have an associated user.

Step 15 (Optional) Associate a user with a user group. Select **User Management** > **User Settings** > **Access Control Group**.

Assigns users a common list of roles and permissions that apply to all users in a user group. Administrators can manage user groups, roles, and permissions to control the level of access (and, therefore, the level of security) for system users.

In order for end users to access the Cisco Unified Communications Self Care Portal, you must add users to the standard Cisco Communications Manager End Users group.

Related Topics

Product Specific Configuration, on page 97
Cisco IP Conference Phone Features and Setup, on page 93
Cisco Unified Communications Manager Documentation, on page 14
Set Up a New Softkey Template, on page 94

Determine the Phone MAC Address

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

Procedure

Perform one of the following actions:

- On the phone, select **Settings** > **Phone Information** and look at the MAC Address field.
- Look at the MAC label on the back of the phone.

- Display the web page for the phone and click **Device Information**.

Phone Addition Methods

After you install the Cisco IP Phone, you can choose one of the following options to add phones to the Cisco Unified Communications Manager database.

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

Before you add phones individually or with BAT, you need the MAC address of the phone. For more information, see Determine the Phone MAC Address, on page 59.

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

Related Topics

Cisco Unified Communications Manager Documentation, on page 14

Add Phones Individually

Collect the MAC address and phone information for the phone that you will add to the Cisco Unified Communications Manager.

Procedure

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

Step 2 Click **Add New**.

Step 3 Select the phone type.

Step 4 Select **Next**.

Step 5 Complete the information about the phone including the MAC Address.

For complete instructions and conceptual information about Cisco Unified Communications Manager, see the documentation for your particular Cisco Unified Communications Manager release.

Step 6 Select **Save**.

Related Topics

Cisco Unified Communications Manager Documentation, on page 14

Add Phones with a BAT Phone Template

The Cisco Unified Communications Bulk Administration Tool (BAT) enables you to perform batch operations, including registration of multiple phones.

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

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

Procedure

Step 1 From Cisco Unified Communications Administration, choose **Bulk Administration** > **Phones** > **Phone Template**.

Step 2 Click **Add New**.

Step 3 Choose a Phone Type and click **Next**.

Step 4 Enter the details of phone-specific parameters, such as Device Pool, Phone Button Template, and Device Security Profile.

Step 5 Click **Save**.

Step 6 Select **Device** > **Phone** > **Add New** to add a phone using the BAT phone template.

Related Topics

Cisco Unified Communications Manager Documentation, on page 14

Add Users to Cisco Unified Communications Manager

You can display and maintain information about the users registered in Cisco Unified Communications Manager. Cisco Unified Communications Manager also allows each user to perform these tasks:

- Access the corporate directory and other customized directories from a Cisco IP Phone.
- Create a personal directory.
- Set up speed dial and call forwarding numbers.
- Subscribe to services that are accessible from a Cisco IP Phone.

Procedure

Step 1 To add users individually, see Add a User Directly to Cisco Unified Communications Manager, on page 62.

Step 2 To add users in batches, use the Bulk Administration Tool. This method also enables you to set an identical default password for all users.

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

Related Topics

Cisco Unified Communications Manager Documentation, on page 14

Add a User from an External LDAP Directory

If you added a user to an LDAP Directory (a non-Cisco Unified Communications Server directory), you can immediately synchronize the LDAP directory to the Cisco Unified Communications Manager on which you are adding the user and the user phone.

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

Procedure

Step 1 Sign into Cisco Unified Communications Manager Administration.

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

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

Step 4 Click on the LDAP directory name.

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

Add a User Directly to Cisco Unified Communications Manager

If you are not using a Lightweight Directory Access Protocol (LDAP) directory, you can add a user directly with Cisco Unified Communications Manager Administration by following these steps.

Note If LDAP is synchronized, you cannot add a user with Cisco Unified Communications Manager Administration.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **User Management** > **End User**.

Step 2 Click **Add New**.

Step 3 In the User Information pane, enter the following:

- User ID: Enter the end user identification name. Cisco Unified Communications Manager does not permit modifying the user ID after it is created. You may use the following special characters: =, +, <, >, #,;, \,, “”, and blank spaces. **Example**: johndoe
- Password and Confirm Password: Enter five or more alphanumeric or special characters for the end user password. You may use the following special characters: =, +, <, >, #, ;, \, , “”, and blank spaces.

- Last Name: Enter the end user last name. You may use the following special characters: =, +, <, >, #, ;, \, , “”, and blank spaces. **Example**: doe
- Telephone Number: Enter the primary directory number for the end user. End users can have multiple lines on their phones. **Example**: 26640 (John Doe’s internal company telephone number)

Step 4 Click **Save**.

Add a User to an End User Group

To add a user to the Cisco Unified Communications Manager Standard End User group, perform these steps:

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **User Management** > **User Settings** > **Access Control Group**.

The Find and List Users window displays.

Step 2 Enter the appropriate search criteria and click **Find**.

Step 3 Select the **Standard CCM End Users** link. The User Group Configuration window for the Standard CCM End Users appears.

Step 4 Select **Add End Users to Group**. The Find and List Users window appears.

Step 5 Use the Find User drop-down list boxes to find the users that you want to add and click **Find**.

A list of users that matches your search criteria appears.

Step 6 In the list of records that appear, click the check box next to the users that you want to add to this user group. If the list is long, use the links at the bottom to see more results.

Note The list of search results does not display users that already belong to the user group.

Step 7 Choose **Add Selected**.

Associate Phones with Users

You associate phones with users from the Cisco Unified Communications Manager End User window.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **User Management** > **End User**.

The Find and List Users window appears.

Step 2 Enter the appropriate search criteria and click **Find**.

Step 3 In the list of records that appear, select the link for the user.

Step 4 Select **Device Association**.

The User Device Association window appears.

Step 5 Enter the appropriate search criteria and click **Find**.

Step 6 Choose the device that you want to associate with the user by checking the box to the left of the device.

Step 7 Choose **Save Selected/Changes** to associate the device with the user.

Step 8 From the Related Links drop-down list in the upper, right corner of the window, select **Back to User**, and click **Go**.

The End User Configuration window appears and the associated devices that you chose display in the Controlled Devices pane.

Step 9 Choose **Save Selected/Changes**.

Survivable Remote Site Telephony

Survivable Remote Site Telephony (SRST) ensures that basic phone functions remain accessible when communications with the controlling Cisco Unified Communications Manager are broken. In this scenario, the phone can keep an in-progress call active, and the user can access a subset of the features available. When failover occurs, the user receives an alert message on the phone.

For information on SRST, see https://www.cisco.com/c/en/us/support/unified-communications/unified-survivable-remote-site-telephony/tsd-products-support-series-home.html

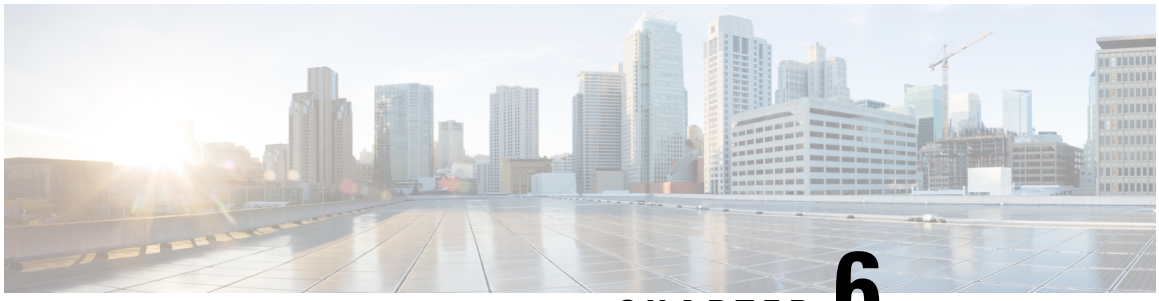
The following table describes the availability of features during failover.

Table 14: SRST Feature Support

Feature	Supported	Notes
New Call	Yes	
End Call	Yes	
Redial	Yes	
Answer	Yes	
Hold	Yes	
Resume	Yes	
Conference	Yes	3 way only and local mixing only.
Conference List	No	
Transfer	Yes	Consult only.
Transfer to Active Calls (Direct Transfer)	No	

Feature	Supported	Notes
Auto Answer	Yes	
Call Waiting	Yes	
Caller ID	Yes	
Unified Session Presentation	Yes	Conference is the only feature supported due to other feature limitations.
Voicemail	Yes	Voicemail will not be synchronized with other users in the Cisco Unified Communications Manager cluster.
Call Forward All	Yes	Forward state is only available on the phone that sets the forward because there are no shared line appearances in SRST mode. The Call Forward All settings are not preserved on failover to SRST from the Cisco Unified Communications Manager, or from SRST fail-back to the Communications Manager. Any original Call Forward All still active on the Communications Manager should be indicated when the device reconnects to the Communications Manager after failover.
Speed Dial	Yes	
To Voicemail (iDivert)	No	The iDivert softkey does not display.
Line Filters	Partial	Lines are supported but cannot be shared.
Park Monitoring	No	The Park softkey does not display.
Enhanced Message Waiting Indication	Yes	Message count badges appear on the phone screen.
Directed Call Park	No	The softkey does not display.
Hold Reversion	Yes	
Remote Hold	No	Calls appear as Local Hold calls.
Meet Me	No	The Meet Me softkey does not display.
PickUp	Yes	
Group PickUp	No	The softkey does not display.
Other PickUp	No	The softkey does not display.
Malicious Call ID	Yes	
QRT	Yes	

Feature	Supported	Notes
Hunt Group	No	The softkey does not display.
Mobility	No	The softkey does not display.
Privacy	No	The softkey does not display.
Call Back	No	The Call Back softkey does not display.
Service URL	Yes	The programmable line key with a Service URL assigned doesn't display.



CHAPTER 6

Self Care Portal Management

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.

Related Topics

Cisco Unified Communications Manager Documentation, on page 14

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

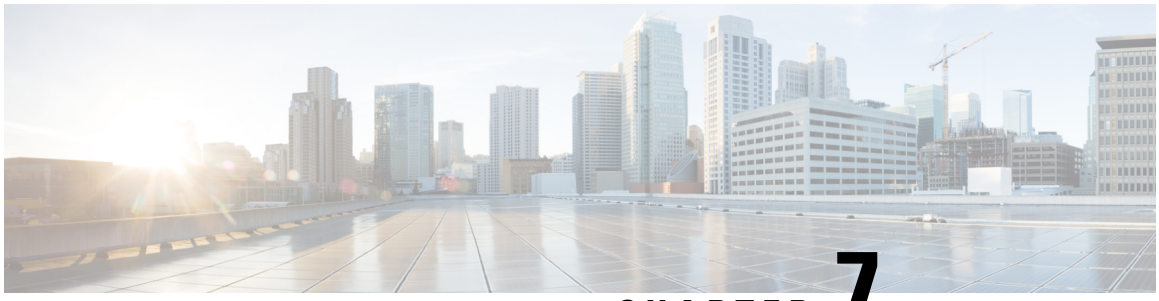
Note The settings apply to all Self Care Portal pages at your site.

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**.

PART III

Cisco IP Conference Phone Administration



CHAPTER 7

Cisco IP Conference Phone Security

Cisco IP Phone Security Overview

The Security features protect against several threats, including threats to the identity of the phone and to data. These features establish and maintain authenticated communication streams between the phone and the Cisco Unified Communications Manager server, and ensure that the phone uses only digitally signed files.

Cisco Unified Communications Manager Release 8.5(1) and later includes Security by Default, which provides the following security features for Cisco IP Phones without running the CTL client:

- Signing of the phone configuration files
- Phone configuration file encryption
- HTTPS with Tomcat and other Web services

Note Secure signaling and media features still require you to run the CTL client and use hardware eTokens.

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

A Locally Significant Certificate (LSC) installs on phones after you perform the necessary tasks that are associated with the Certificate Authority Proxy Function (CAPF). You can use Cisco Unified Communications Manager Administration to configure an LSC. For more information, see the documentation for your particular Cisco Unified Communications Manager release.

A LSC cannot be used as the user certificate for EAP-TLS with WLAN authentication.

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

The Cisco IP Conference Phone 8832 complies with Federal Information Processing Standard (FIPS). To function correctly, FIPS mode requires an RSA key size of 2048 bits or greater. If the RSA server certificate is not 2048 bits or greater, the phone will not register with Cisco Unified Communications Manager and

`Phone failed to register. Cert key size is not FIPS compliant` displays in the phone's status messages.

You cannot use private keys (LSC or MIC) in FIPS mode.

If the phone has an existing LSC that is smaller than 2048 bits, you need to update the LSC key size to 2048 bits or greater before enabling FIPS.

Related Topics

Set Up a Locally Significant Certificate, on page 76
Cisco Unified Communications Manager Documentation, on page 14

Security Enhancements for Your Phone Network

You can enable Cisco Unified Communications Manager 11.5(1) or later version to operate in an enhanced security environment. With these enhancements, your phone network operates under a set of strict security and risk management controls to protect you and your users.

The enhanced security environment includes the following features:

- Contact search authentication.
- TCP as the default protocol for remote audit logging.
- FIPS mode.
- An improved credentials policy.
- Support for the SHA-2 family of hashes for digital signatures.
- Support for a RSA key size of 512 and 4096 bits.

Note Your Cisco IP Phone can only store a limited number of Identity Trust List (ITL) files. ITL files cannot exceed 64K limit on phone so limit the number of files that the Cisco Unified Communications Manager sends to the phone.

SIP OAuth Support

SIP OAuth mode allows you to use OAuth refresh tokens for phone authentication.

Cisco Unified Communications Manager (Unified CM) verifies the token presented by the phone and serves the configuration files only to authorized ones. OAuth token validation during SIP registration is completed when OAuth-based authorization is enabled on Unified CM cluster and Cisco IP phones.

Cisco IP phones support SIP OAuth authentication on Proxy Trivial File Transfer Protocol (TFTP) and Cisco Unified Survivable Remote Site Telephony (SRST).

- SIP OAuth on TFTP requirements:
  - Cisco Unified Communications Manager Release 14.0(1)SU1 or later
  - Cisco IP Phone Firmware Release 14.1(1) or later

Note Proxy TFTP and OAuth for Proxy TFTP aren't supported on Mobile Remote Access (MRA).

- SIP OAuth on SRST requirements:
  - Cisco Unified Communications Manager 14.0(1)SU1 or later
  - Cisco IP Phone Firmware Release 14.2(1) or later
  - Cisco SRST Software Release: IOS XE 17.8.1a or later
  - Cisco SRST Hardware Models: ISR1100, ISR43xx, ISR44xx, Catalyst 8200, or Catalyst 8300 platform

For information about how to configure SIP OAuth, see **SIP OAuth Mode** in *Security Guide for Cisco Unified Communications Manager*.

Where to Find More Information about Phone Security

For additional information about security, see the following:

- *Security Guide for Cisco Unified Communications Manager* (https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/security/14SU2/cucm_b_security-guide-14su2.html)
- *Cisco Unified SCCP and SIP SRST System Administration Guide* (https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cusrst/admin/sccp_sip_srst/configuration/guide/SCCP_and_SIP_SRST_Admin_Guide/srst_roadmap.html)
- *System Configuration Guide for Cisco Unified Communications Manager*, Release 14.0(1) or later (https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html).

Supported Security Features

Security features protect against several threats, including threats to the identity of the phone and to data. These features establish and maintain authenticated communication streams between the phone and the Cisco Unified Communications Manager server, and ensure that the phone uses only digitally signed files.

Cisco Unified Communications Manager Release 8.5(1) and later includes Security by Default, which provides the following security features for Cisco IP Phones without running the CTL client:

- Signing of the phone configuration files
- Phone configuration file encryption
- HTTPS with Tomcat and other Web services

Note Secure signaling and media features still require you to run the CTL client and use hardware eTokens.

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

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

A Locally Significant Certificate (LSC) installs on phones after you perform the necessary tasks that are associated with the Certificate Authority Proxy Function (CAPF). You can use Cisco Unified Communications Manager Administration to configure an LSC, as described in the Cisco Unified Communications Manager Security Guide. Alternatively, you can initiate the installation of an LSC from the Security Setup menu on the phone. This menu also lets you update or remove an LSC.

A LSC cannot be used as the user certificate for EAP-TLS with WLAN authentication.

The phones use the phone security profile, which defines whether the device is nonsecure or secure. For information about applying the security profile to the phone, see the documentation for your particular Cisco Unified Communications Manager release.

If you configure security-related settings in Cisco Unified Communications Manager Administration, the phone configuration file contains sensitive information. To ensure the privacy of a configuration file, you must configure it for encryption. For detailed information, see the documentation for your particular Cisco Unified Communications Manager release.

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

The following table provides an overview of the security features that the Cisco IP Conference Phone 8832 supports. For more information about these features, Cisco Unified Communications Manager, and Cisco IP Phone security, see the documentation for your particular Cisco Unified Communications Manager release.

Table 15: Overview of Security Features

Feature	Description
Image authentication	Signed binary files (with the extension .sbn) prevent tampering image causes a phone to fail the authentication process and rej
Customer-site certificate installation	Each phone requires a unique certificate for device authenticatio security, you can specify in Cisco Unified Communications M Authority Proxy Function (CAPF). Alternatively, you can insta on the phone.
Device authentication	Occurs between the Cisco Unified Communications Manager s Determines whether a secure connection between the phone ar creates a secure signaling path between the entities by using T unless they can be authenticated by the Cisco Unified Commu
File authentication	Validates digitally signed files that the phone downloads. The after the file creation. Files that fail authentication are not writt processing.
Signaling Authentication	Uses the TLS protocol to validate that no tampering has occur

Feature	Description
Manufacturing installed certificate	Each phone contains a unique manufacturing installed cert unique proof of identity for the phone, and allows Cisco U
Secure SRST reference	After you configure a SRST reference for security and ther Administration, the TFTP server adds the SRST certificate a TLS connection to interact with the SRST-enabled router
Media encryption	Uses SRTP to ensure that the media streams between supp the data. Includes creating a media primary key pair for the while the keys are in transport.
CAPF (Certificate Authority Proxy Function)	Implements parts of the certificate generation procedure th generation and certificate installation. The CAPF can be co behalf of the phone, or it can be configured to generate cer
Security profiles	Defines whether the phone is nonsecure, authenticated, or
Encrypted configuration files	Lets you ensure the privacy of phone configuration files.
Optional disabling of the web server functionality for a phone	You can prevent access to a phone web page, which displa
Phone hardening	Additional security options, which you control from Cisco • Disable access to web pages for a phone **Note** You can view current settings for the GARP E menu.
802.1X Authentication	The phone can use 802.1X authentication to request and ga
AES 256 Encryption	When connected to Cisco Unified Communications Manag TLS and SIP for signaling and media encryption. This enabl that conform to SHA-2 (Secure Hash Algorithm) standards ciphers are: • For TLS connections: • TLS_ECDHE_RSA_WITH_AES_256_GCM_S • TLS_ECDHE_RSA_WITH_AES_128_GCM_S • For sRTP: • AEAD_AES_256_GCM • AEAD_AES_128_GCM For more information, see the Cisco Unified Communicati
Elliptic Curve Digital Signature Algorithm (ECDSA) certificates	As part of Common Criteria (CC) certification, Cisco Unifie all Voice Operating System (VOS) products from version

Related Topics

Cisco Unified Communications Manager Documentation, on page 14

Set Up a Locally Significant Certificate

This task applies to setting up a LSC with the authentication string method.

Before you begin

Make sure that the appropriate Cisco Unified Communications Manager and the Certificate Authority Proxy Function (CAPF) security configurations are complete:

- The CTL or ITL file has a CAPF certificate.
- In Cisco Unified Communications Operating System Administration, verify that the CAPF certificate is installed.
- The CAPF is running and configured.

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

Procedure

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

Step 2 From the phone, choose **Settings**.

Step 3 Choose **Admin Settings** > **Security Setup**.

Note You can control access to the Settings menu by using the Settings Access field in the Cisco Unified Communications Manager Administration Phone Configuration window.

Step 4 Choose **LSC** and press **Select** or **Update**.

The phone prompts for an authentication string.

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

The phone begins to install, update, or remove the LSC, depending on how the CAPF is configured. During the procedure, a series of messages appears in the LSC option field in the Security Configuration menu, so you can monitor progress. When the procedure is complete, Installed or Not Installed displays on the phone.

The LSC install, update, or removal process can take a long time to complete.

When the phone installation procedure is successful, the `Installed` message displays. If the phone displays `Not Installed`, then the authorization string may be incorrect or the phone upgrade may not be enabled. If the CAPF operation deletes the LSC, the phone displays `Not Installed` to indicate that the operation succeeded. The CAPF server logs the error messages. See the CAPF server documentation to locate the logs and to understand the meaning of the error messages.

Related Topics

Cisco Unified Communications Manager Documentation, on page 14

Enable FIPS Mode

Procedure

Step 1 In Cisco Unified Communications Manager Administration, select **Device** > **Phone** and locate the phone.
Step 2 Navigate to the Product Specific Configuration area.
Step 3 Set the **FIPS Mode** field to Enabled.
Step 4 Select **Apply Config**.
Step 5 Select **Save**.
Step 6 Restart the phone.

Phone Call Security

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

In a secure call, all call signaling and media streams are encrypted. A secure call offers a high level of security, providing integrity and privacy to the call. When a call in progress is encrypted, the call progress icon to the right of the call duration timer in the phone screen changes to the following icon:  .

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

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

Note Secure calling is supported between two phones. Secure conference, Cisco Extension Mobility, and shared lines can be configured by a secure conference bridge.

When a phone is configured as secure (encrypted and trusted) in Cisco Unified Communications Manager, it can be given a “protected” status. After that, if desired, the protected phone can be configured to play an indication tone at the beginning of a call:

- Protected Device: To change the status of a secure phone to protected, check the Protected Device check box in the Phone Configuration window in Cisco Unified Communications Manager Administration (**Device** > **Phone**).
- Play Secure Indication Tone: To enable the protected phone to play a secure or nonsecure indication tone, set the Play Secure Indication Tone setting to True. By default, Play Secure Indication Tone is set to False. You set this option in Cisco Unified Communications Manager Administration (**System** > **Service Parameters**). Select the server and then the Unified Communications Manager service. In the

Service Parameter Configuration window, select the option in the Feature - Secure Tone area. The default is False.

Secure Conference Call Identification

You can initiate a secure conference call and monitor the security level of participants. A secure conference call is established by using this process:

1. A user initiates the conference from a secure phone.
2. Cisco Unified Communications Manager assigns a secure conference bridge to the call.
3. As participants are added, Cisco Unified Communications Manager verifies the security mode of each phone and maintains the secure level for the conference.
4. The phone displays the security level of the conference call. A secure conference displays the secure icon  to the right of **Conference** on the phone screen.

Note Secure calling is supported between two phones. For protected phones, some features, such as conference calling, shared lines, and Extension Mobility, are not available when secure calling is configured.

The following table provides information about changes to conference security levels depending on the initiator phone security level, the security levels of participants, and the availability of secure conference bridges.

Table 16: Security Restrictions with Conference Calls

Initiator Phone Security Level	Feature Used	Security Level of Participants	Results of Action
Nonsecure	Conference	Secure	Nonsecure conference bridge Nonsecure conference
Secure	Conference	At least one member is nonsecure.	Secure conference bridge Nonsecure conference
Secure	Conference	Secure	Secure conference bridge Secure encrypted level conference
Nonsecure	Meet Me	Minimum security level is encrypted.	Initiator receives message `Does not meet Security Level, call rejected`.
Secure	Meet Me	Minimum security level is nonsecure.	Secure conference bridge Conference accepts all calls.

Secure Phone Call Identification

A secure call is established when your phone, and the phone on the other end, is configured for secure calling. The other phone can be in the same Cisco IP network, or on a network outside the IP network. Secured calls

can only be made between two phones. Conference calls should support secure call after secure conference bridge set up.

A secured call is established using this process:

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

Note Secure calling is supported between two phones. For protected phones, some features, such as conference calling, shared lines, and Extension Mobility, are not available when secure calling is configured.

Only protected phones play these secure or nonsecure indication tones. Nonprotected phones never play tones. If the overall call status changes during the call, the indication tone changes and the protected phone plays the appropriate tone.

A protected phone plays a tone or not under these circumstances:

- When the Play Secure Indication Tone option is enabled:
  - When end-to-end secure media is established and the call status is secure, the phone plays the secure indication tone (three long beeps with pauses).
  - When end-to-end nonsecure media is established and the call status is nonsecure, the phone plays the nonsecure indicationtone (six short beeps with brief pauses).

If the Play Secure Indication Tone option is disabled, no tone plays.

Provide Encryption for Barge

Cisco Unified Communications Manager checks the phone security status when conferences are established and changes the security indication for the conference or blocks the completion of the call to maintain integrity and security in the system.

A user cannot barge into an encrypted call if the phone that is used to barge is not configured for encryption. When barge fails in this case, a reorder (fast busy) tone plays on the phone that the barge was initiated.

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

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

WLAN Security

Because all WLAN devices that are within range can receive all other WLAN traffic, securing voice communications is critical in WLANs. To ensure that intruders do not manipulate nor intercept voice traffic,

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

The Cisco Wireless IP telephony solution provides wireless network security that prevents unauthorized sign-ins and compromised communications by using the following authentication methods that the wireless Cisco IP Phone supports:

- Open Authentication: Any wireless device can request authentication in an open system. The AP that receives the request may grant authentication to any requestor or only to requestors that are found on a list of users. Communication between the wireless device and AP could be nonencrypted or devices can use Wired Equivalent Privacy (WEP) keys to provide security. Devices that use WEP only attempt to authenticate with an AP that is using WEP.
- Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) Authentication: This client server security architecture encrypts EAP transactions within a Transport Level Security (TLS) tunnel between the AP and the RADIUS server, such as the Cisco Access Control Server (ACS).

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

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

- Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) Authentication: EAP-TLS requires a client certificate for authentication and network access. For wired EAP-TLS, the client certificate can be either the phone's MIC or an LSC. LSC is the recommended client authentication certificate for wired EAP-TLS.
- Protected Extensible Authentication Protocol (PEAP): Cisco proprietary password-based mutual authentication scheme between the client (phone) and a RADIUS server. Cisco IP Phone can use PEAP for authentication with the wireless network. Only PEAP-MSCHAPV2 is supported. PEAP-GTC is not supported.

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 preshared keys that are stored on the AP and phone.
- Fast Secure Roaming: 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. The Cisco IP Phone 8800 Series supports 802.11r (FT). Both 11r (FT) and CCKM are supported to allow for fast secure roaming. But Cisco strongly recommends to utilize the 802.11r (FT) over air method.

With WPA/WPA2 and CCKM, encryption keys are not entered on the phone, but are automatically derived between the AP and phone. But the EAP username and password that are used for authentication must be entered on each phone.

To ensure that voice traffic is secure, the Cisco IP Phone supports WEP, TKIP, and Advanced Encryption Standards (AES) for encryption. When these mechanisms are used for encryption, both the signalling SIP packets and voice Real-Time Transport Protocol (RTP) packets are encrypted between the AP and the Cisco IP Phone.

WEP

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

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

TKIP

WPA and CCKM use TKIP encryption that has several improvements over WEP. TKIP provides per-packet key ciphering and longer initialization vectors (IVs) that strengthen encryption. In addition, a message integrity check (MIC) ensures that encrypted packets are not being altered. TKIP removes the predictability of WEP that helps intruders decipher the WEP key.

AES

An encryption method used for WPA2 authentication. This national standard for encryption uses a symmetrical algorithm that has the same key for encryption and decryption. AES uses Cipher Blocking Chain (CBC) encryption of 128 bits in size, which supports key sizes of 128, 192 and 256 bits, as a minimum. The Cisco IP Phone supports a key size of 256 bits.

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

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 client devices to authenticate successfully, you must configure the same SSIDs with their authentication and encryption schemes on the APs and on the Cisco IP Phone.

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

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 Cisco IP Phone does 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 Cisco IP Phone supports. The table shows the network configuration option for the phone that corresponds to the AP configuration.

Table 17: Authentication and Encryption Schemes

Cisco IP Phone Configuration	**AP Configuration**			
Security Mode	Security	Key Management	Encryption	Fast Roaming
None	None	None	None	N/A
WEP	Static WEP	Static	WEP	N/A
PSK	PSK	WPA	TKIP	None
		WPA2	AES	FT
EAP-FAST	EAP-FAST	802.1x	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM
EAP-TLS	EAP-TLS	802.1x	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM
PEAP-MSCHAPV2	PEAP-MSCHAPV2	802.1x	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM

For more information about configuring authentication and encryption schemes on APs, see the *Cisco Aironet Configuration Guide* for your model and release under the following URL:

http://www.cisco.com/cisco/web/psa/configure.html?mode=prod&level0=278875243

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*.

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.

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** section, set **Web Admin** to **Enabled**.

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.

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**.

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 Browse to the certificate on your PC.

Step 3 In the **Extract password** field, enter the certificate extract password.

Step 4 Click **Upload**.

Step 5 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.

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 & Time**.

Step 2 Perform one of the following options:

- Click **Set Phone to Local Date & Time** to synch the phone to a local server.
- In the **Specify Date & Time** fields, select the month, day, year, hour, minute, and second using the menus and click **Set Phone to Specific Date & Time**.

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.

802.1x Authentication

The Cisco IP Phones support 802.1X Authentication.

Cisco IP Phones and Cisco Catalyst switches traditionally use Cisco Discovery Protocol (CDP) to identify each other and determine parameters such as VLAN allocation and inline power requirements.

Support for 802.1X authentication requires several components:

- Cisco IP Phone: The phone initiates the request to access the network. Phones contain an 802.1X supplicant. This supplicant allows network administrators to control the connectivity of IP phones to the LAN switch ports. The current release of the phone 802.1X supplicant uses the EAP-FAST and EAP-TLS options for network authentication.
- Cisco Catalyst Switch (or other third-party switch): The switch must support 802.1X, so it can act as the authenticator and pass the messages between the phone and the authentication server. After the exchange completes, the switch grants or denies the phone access to the network.

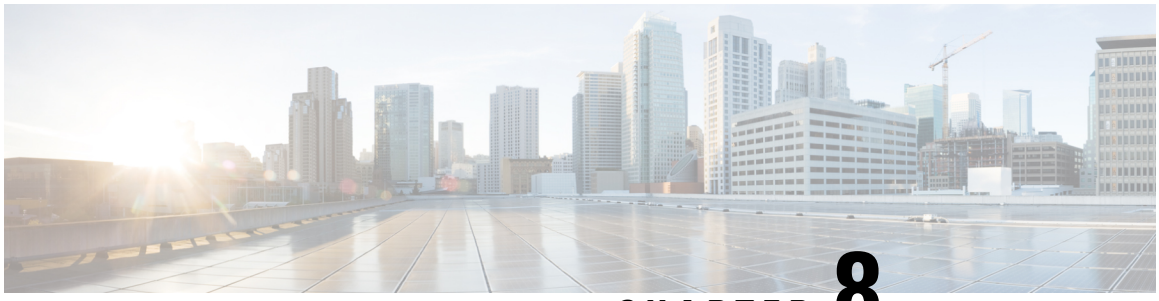
You must perform the following actions to configure 802.1X.

- Configure the other components before you enable 802.1X Authentication on the phone.
- Configure Voice VLAN—Because the 802.1X standard does not account for VLANs, you should configure this setting based on the switch support.

- Enabled—If you are using a switch that supports multidomain authentication, you can continue to use the voice VLAN.
- Disabled—If the switch does not support multidomain authentication, disable the Voice VLAN and consider assigning the port to the native VLAN.

Related Topics

Cisco Unified Communications Manager Documentation, on page 14



CHAPTER 8

Cisco IP Conference Phone Customization

Custom Phone Ringtones

The Cisco IP Phone ships with two default ringtones that are implemented in hardware: Chirp1 and Chirp2. Cisco Unified Communications Manager also provides a default set of additional phone ringtones that are implemented in software as pulse code modulation (PCM) files. The PCM files, along with an XML file 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 the wrong case 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.

Related Topics

Cisco Unified Communications Manager Documentation, on page 14

Set Up a Custom Phone Ring

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 the Custom Ring File Formats section.

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 Save your modifications and close the Ringlist-wb file.

Step 4 To cache the new Ringlist-wb file:

- Stop and start the TFTP service by using Cisco Unified Serviceability
- Disable and reenable the "Enable Caching of Constant and Bin Files at Startup" TFTP service parameter, located in the Advanced Service Parameters area.

Related Topics

Cisco Unified Communications Manager Documentation, on page 14

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 Cisco IP 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 Cisco IP 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 Cisco IP 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.

Customize the Dial Tone

You can set up your phones so that users hear different dial tones for internal and external calls. Depending upon your needs, you can choose from three dial tone options:

- Default: A different dial tone for inside and outside calls.
- Inside: The inside dial tone is used for all calls.
- Outside: The outside dial tone is used for all calls.

Always Use Dial Tone is a required field on Cisco Unified Communications Manager.

Procedure

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

Step 2 Select the appropriate Server.

Step 3 Select **Cisco CallManager** as the Service.

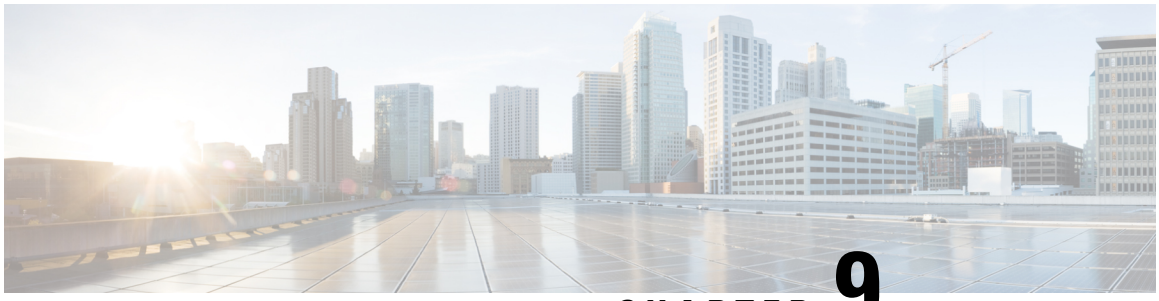
Step 4 Scroll to the Clusterwide Parameters pane.

Step 5 Set **Always Use Dial Tone** to one of the following:

- Outside
- Inside
- Default

Step 6 Select **Save**.

Step 7 Restart your phones.



CHAPTER 9

Cisco IP Conference Phone Features and Setup

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

Migration of your Phone to a Multiplatform Phone Directly

You can migrate your enterprise phone to a multiplatform phone easily in one step without using transition firmware load. All you need is to obtain and authorize the migration license from the server.

For more information, see https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/MPP/MPP-conversion/enterprise-to-mpp/cuip_b_conversion-guide-ipphone.html

Set Up a New Softkey Template

You need to add softkeys to a softkey template to give users access to some features. For example, if you want users to be able to use do not disturb, you need to enable the softkey. For more information, see the documentation for your particular Cisco Unified Communications Manager release.

You may want to create several templates. For example, you might want a template for the phone in a conference room, and another template for a phone in an executive's office.

This procedure takes you through the steps to create a new softkey template and assign it to a specific phone. Similar to other phone features, you can also use the template for all your conference phones or a group of phones.

Procedure

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

Step 2 Select **Device** > **Device Settings** > **Softkey Template**.

Step 3 Click **Find**.

Step 4 Select one of the following options:

- Cisco Unified Communications Manager 11.5 and previous releases—**Standard User**
- Cisco Unified Communications Manager 12.0 and later releases—**Personal Conference User** or **Public Conference User**.

Step 5 Click **Copy**.

Step 6 Change the name of the template.

For example, 8832 Conference Room Template.

Step 7 Click **Save**.

Step 8 Go to the **Configure Softkey Layout** page from the top right menu.

Step 9 For each call state, set the features to display.

Step 10 Click **Save**.

Step 11 Return to the **Find/List screen** from the top right menu.

You see your new template in the list of templates.

Step 12 Select **Device** > **Phone**.

Step 13 Find the phone to have the new template and select it.

Step 14 In the **Softkey Template** field, select the new softkey template.

Step 15 Click **Save** and **Apply Config**.

Related Topics

Cisco Unified Communications Manager Documentation, on page 14

Configure Phone Services for Users

You can give users access to Cisco IP Phone Services on the IP phone. You can also assign a button to different phone services. The IP phone manages each service as a separate application.

Before a user can access any service:

- Use Cisco Unified Communications Manager Administration to configure services that are not present by default.
- The user must subscribe to services by using the Cisco Unified Communications Self Care Portal. This web-based application provides a graphical user interface (GUI) for limited, end-user configuration of IP phone applications. However, a user cannot subscribe to any service that you configure as an enterprise subscription.

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

Before you set up services, gather the URLs for the sites that you want to set up and verify that users can access those sites from your corporate IP telephony network. This activity is not applicable for the default services that Cisco provides.

Procedure

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

Step 2 Verify that your users can access the Cisco Unified Communications Self Care Portal, from which they can select and subscribe to configured services.

See Self Care Portal Overview, on page 67 for a summary of the information that you must provide to end users.

Related Topics

Cisco Unified Communications Manager Documentation, on page 14

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.

Related Topics

Configure User Credentials Persistent for Expressway Sign-In, on page 119

Set Up Phone Features for All Phones

Procedure

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

Step 2 Select **System** > **Enterprise Phone Configuration**.

Step 3 Set the fields you want to change.

Step 4 Check the **Override Enterprise Settings** check box for any changed fields.

Step 5 Click **Save**.

Step 6 Click **Apply Config**.

Step 7 Restart the phones.

Note This will impact all phones in your organization.

Related Topics

Product Specific Configuration, on page 97

Set Up Phone Features for a Group of Phones

Procedure

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

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

Step 3 Locate the profile.
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, on page 97

Set Up Phone Features for a Single Phone

Procedure

Step 1 Sign in to 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, on page 97

Product Specific Configuration

The following table describes the fields in the Product Specific Configuration Layout pane. Some fields in this table only display in the **Device** > **Phone** page.

Table 18: Product Specific Configuration Fields

Field Name	Field Type Or Choices	Default	Description
Settings Access	Disabled Enabled Restricted	Enabled	Enables, disables, or restricts access to local configuration settings in the Settings app. With restricted access, the Preferences and System 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.

Field Name	Field Type Or Choices	Default	Description
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.
Web Access	Disabled Enabled	Disabled	Enables or disables access to the phone web pages through a web browser. **Caution** If you enable this field, you may expose sensitive information about the phone.
Disable TLS 1.0 and TLS 1.1 for WebAccess	Disabled Enabled	Enabled	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 a HTTPs server. • Enabled—Only a phone configured for TLS1.2 can function as a HTTPs server.
Enbloc Dialing	Disabled Enabled	Disabled	Controls the dialing method. • Disabled—The Cisco Unified Communications Manager waits for the interdigit timer to expire when there is a dial plan or route pattern overlap. • Enabled—The entire dialed string is sent to Cisco Unified Communications Manager once the dialing is complete. To avoid the T.302 timer timeout, we recommend that you enable Enbloc dialing whenever there is a dialplan or route pattern overlap. Forced Authorization Codes (FAC) or Client Matter Codes (CMC) do not support the Enbloc Dialing. If you use FAC or CMC to manage call access and accounting, then you cannot use this feature.
Days Backlight Not Active	Days of the week		Defines the days that the backlight does not turn on automatically at the time specified in the Backlight On Time field. Choose the day or days from the drop-down list. To choose more than one day, **Ctrl+click** each day that you want. See Schedule Power Save for Cisco IP Phone, on page 109.

Field Name	Field Type Or Choices	Default	Description
Backlight On Time	hh:mm		Defines the time each day that the backlight turns on automatically (except on the days specified in the Backlight Display Not Active field). Enter the time in this field in 24 hour format, where 0:00 is midnight. For example, to automatically turn the backlight on at 07:00 a.m. (0700), enter 07:00. To turn the backlight on at 02:00 p.m. (1400), enter 14:00. If this field is blank, the backlight automatically turns on at 0:00. See Schedule Power Save for Cisco IP Phone, on page 109.
Backlight On Duration	hh:mm		Defines the length of time that the backlight remains on after turning on at the time specified in the Backlight On Time field. For example, to keep the backlight on for 4 hours and 30 minutes after it turns on automatically, enter 04:30. If this field is blank, the phone turns off at the end of the day (0:00). If Backlight On Time is 0:00 and the backlight on duration is blank (or 24:00), the backlight does not turn off. See Schedule Power Save for Cisco IP Phone, on page 109.
Backlight Idle Timeout	hh:mm		Defines the length of time that the phone is idle before the backlight turns off. Applies only when the backlight was off as scheduled and was turned on by a user (by pressing a button on the phone or lifting the handset). For example, to turn the backlight off when the phone is idle for 1 hour and 30 minutes after a user turns the backlight on, enter 01:30. See Schedule Power Save for Cisco IP Phone, on page 109.
Backlight On When Incoming Call	Disabled Enabled	Enabled	Turns the backlight on when there is an incoming call.

Field Name	Field Type Or Choices	Default	Description
Enable Power Save Plus	Days of the week		Defines the schedule of days for which the phone powers off. Choose the day or days from the drop-down list. To choose more than one day, **Ctrl+click** each day that you want. When Enable Power Save Plus is turned on, you receive a message that warns about emergency (e911) concerns. **Caution** While Power Save Plus Mode (the "Mode") is in effect, endpoints that are configured for the mode are disabled for emergency calling and from receiving inbound calls. By selecting this mode, you agree to the following: (i) You take full responsibility for providing alternate methods for emergency calling and receiving calls while the mode is in effect; (ii) Cisco has no liability in connection with your selection of the mode and all liability in connection with enabling the mode is your responsibility; and (iii) You fully inform users of the effects of the mode on calls, calling and otherwise. To disable Power Save Plus, you must uncheck the Allow EnergyWise Overrides check box. If the Allow EnergyWise Overrides remains checked but no days are selected in the Enable Power Save Plus field, Power Save Plus is not disabled. See Schedule EnergyWise on Cisco IP Phone, on page 110.

Field Name	Field Type Or Choices	Default	Description
Phone On Time	hh:mm		Determines when the phone automatically turns on for the days that are in the Enable Power Save Plus field. Enter the time in this field in 24-hour format, where 00:00 is midnight. For example, to automatically power up the phone at 07:00 a.m. (0700), enter 07:00. To power up the phone at 02:00 p.m. (1400), enter 14:00. The default value is blank, which means 00:00. The Phone On Time must be at least 20 minutes later than the Phone Off Time. For example, if the Phone Off Time is 07:00, the Phone On Time must be no earlier than 07:20. See Schedule EnergyWise on Cisco IP Phone, on page 110.
Phone Off Time	hh:mm		Defines the time of day that the phone powers down for the days that are selected in the Enable Power Save Plus field. If the Phone On Time and the Phone Off Time fields contain the same value, the phone does not power down. Enter the time in this field in 24-hour format, where 00:00 is midnight. For example, to automatically power down the phone at 7:00 a.m. (0700), enter 7:00. To power down the phone at 2:00 p.m. (1400), enter 14:00. The default value is blank, which means 00:00. The Phone On Time must be at least 20 minutes later than the Phone Off Time. For example, if the Phone Off Time is 7:00, the Phone On Time must be no earlier than 7:20. See Schedule EnergyWise on Cisco IP Phone, on page 110.

Field Name	Field Type Or Choices	Default	Description
Phone Off Idle Timeout	hh:mm		Indicates the length of time that the phone must be idle before the phone powers down. The timeout occurs under the following conditions: • When the phone was in Power Save Plus mode, as scheduled, and was taken out of Power Save Plus mode because the phone user pressed the Select key. • When the phone is repowered by the attached switch. • When the Phone Off Time is reached but the phone is in use. See Schedule EnergyWise on Cisco IP Phone, on page 110.
Enable Audible Alert	Checkbox	Unchecked	When enabled, instructs the phone to play an audible alert starting 10 minutes before the time that the Phone Off Time field specifies. This check box applies only if the Enable Power Save Plus list box has one or more days selected. See Schedule EnergyWise on Cisco IP Phone, on page 110.
EnergyWise Domain	Up to 127 characters		Identifies the EnergyWise domain that the phone is in. See Schedule EnergyWise on Cisco IP Phone, on page 110.
EnergyWise Secret	Up to 127 characters		Identifies the security secret password that is used to communicate with the endpoints in the EnergyWise domain. See Schedule EnergyWise on Cisco IP Phone, on page 110.

Field Name	Field Type Or Choices	Default	Description
Allow EnergyWise Overrides	Check box	Unchecked	Determines whether you allow the EnergyWise domain controller policy to send power level updates to the phones. The following conditions apply: • One or more days must be selected in the Enable Power Save Plus field. • The settings in Cisco Unified Communications Manager Administration take effect on schedule even if EnergyWise sends an override. For example, assuming the Phone Off Time is set to 22:00 (10:00 p.m.), the value in the Phone On Time field is 06:00 (6:00 a.m.), and the Enable Power Save Plus has one or more days selected. • If EnergyWise directs the phone to turn off at 20:00 (8:00 p.m.), that directive remains in effect (assuming no phone user intervention occurs) until the configured Phone On Time at 6:00 a.m. • At 6:00 a.m., the phone turns on and resumes receiving the power level changes from the settings in Cisco Unified Communications Manager Administration. • To change the power level on the phone again, EnergyWise must reissue a new power level change command. To disable Power Save Plus, you must uncheck the Allow EnergyWise Overrides check box. If the Allow EnergyWise Overrides remains checked but no days are selected in the Enable Power Save Plus field, Power Save Plus is not disabled. See Schedule EnergyWise on Cisco IP Phone, on page 110.
Join And Direct Transfer Policy	Same line enable Same line disable	Same line, across line enable	Controls the ability of a user to join and transfer calls. • Same line enable—Users can directly transfer or join a call on the current line to another call on the same line. • Same line disable— Users can't join or transfer calls on the same line. The join and transfer features are disabled and the user can't do the direct transfer or join function.

Field Name	Field Type Or Choices	Default	Description
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.
Log Server	String of up to 256 characters		Identifies the IPv4 syslog server for phone debug output. The format for the address is: `address:<port>@@base=<0-7>;pfs=<0-1>`
Remote Log	Disabled Enabled	Disabled	Controls the ability to send logs to the syslog server.
Log Profile	Default Preset Telephony SIP UI Network Media Upgrade Accessory Security Energywise MobileRemoteAccess	Preset	Specifies the predefined logging profile. • Default—Default debug logging level • Preset—Does not overwrite the phone local debug logging setting • Telephony—Logs information about Telephony or call features • SIP—Logs information about SIP signaling • UI—Logs information about the phone user interface • Network—Logs network information • Media—Logs media information • Upgrade—Logs upgrade information • Accessory—Logs accessory information • Security—Logs security information • Energywise—Logs energy-savings information • MobileRemoteAccess—Logs Mobile and Remote Access through Expressway information
IPv6 Log Server	String of up to 256 characters		Identifies the IPv6 syslog server for phone debug output.

Field Name	Field Type Or Choices	Default	Description
Cisco Discovery Protocol (CDP): Switch Port	Disabled Enabled	Enabled	Controls Cisco Discovery Protocol on the phone.
Link Layer Discovery Protocol - Media Endpoint Discover (LLDP-MED): Switch Port	Disabled Enabled	Enabled	Enables LLDP-MED on the SW port.
LLDP Asset ID	String, up to 32 characters		Identifies the asset ID that is assigned to the phone for inventory management.
Energy Efficient Ethernet(EEE): Switch Port	Disabled Enabled	Disabled	Controls EEE on the switch port.
LLDP Power Priority	Unknown Low High Critical	Unknown	Assigns a phone power priority to the switch, thus enabling the switch to appropriately provide power to the phones.
802.1x Authentication	User Controlled Disabled Enabled	User Controlled	Specifies the 802.1x authentication feature status. • User Controlled—The user can configure the 802.1x on the phone. • Disabled—802.1x authentication is not used. • Enabled—802.1x authentication is used, and you configure the authentication for the phones.
Switch Port Remote Configuration	Disabled Auto Negotiate 10 Half 10 Full 100 Half 100 Full	Disabled	Allows you to configure the speed and duplex function of the phone SW port remotely. This enhances the performance for large deployments with specific port settings. If the SW ports are configured for Remote Port Configuration in Cisco Unified Communications Manager, the data cannot be changed 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.

Field Name	Field Type Or Choices	Default	Description
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.
FIPS Mode	Disabled Enabled	Disabled	Enables or disables the Federal Information Processing Standards (FIPS) mode on the phone.
Record Call Log from Shared Line	Disabled Enabled	Disabled	Specifies whether to record call log from a shared line.
Minimum Ring Volume	0 - Silent 1–15	0 - Silent	Controls the minimum ring volume for the phone.
Peer Firmware Sharing	Disabled Enabled	Enabled	Allows the phone to find other phones of the same model on the subnet and share updated firmware files. If the phone has a new firmware load, it can share that load with the other phones. If one of the other phones has a new firmware load, the phone can download the firmware from the other phone, instead of from the TFTP server. Peer firmware sharing: • Limits congestion on TFTP transfers to centralized remove TFTP servers. • Eliminates the need to manually control firmware upgrades. • Reduces phone downtime during upgrades when large numbers of phones are reset simultaneously. • Helps with firmware upgrades in branch or remote office deployment scenarios that run over bandwidth-limited WAN links.
Load Server	String of up to 256 characters		Identifies the alternate IPv4 server that the phone uses to obtain firmware loads and upgrades.
IPv6 Load Server	String of up to 256 characters		Identifies the alternate IPv6 server that the phone uses to obtain firmware loads and upgrades.

Field Name	Field Type Or Choices	Default	Description
Detect Unified CM Connection Failure	Normal Delayed	Normal	Determines the sensitivity that the phone has for detecting a connection failure to Cisco Unified Communications Manager (Unified CM), which is the first step before device failover to a backup Unified CM/SRST occurs. Valid values specify Normal (detection of a Unified CM connection failure occurs at the standard system rate) or Delayed (detection of a Unified CM connection failover occurs approximately four times slower than Normal). For faster recognition of a Unified CM connection failure, choose Normal. If you prefer failover to be delayed slightly to give the connection the opportunity to reestablish, choose Delayed. The precise time difference between Normal and Delayed connection failure detection depends on many variables that are constantly changing.
Special Requirement ID	String		Controls custom features from Engineering Special (ES) loads.
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.
User Credentials Persistent for Expressway Sign in	Disabled Enabled	Disabled	Controls if the phone stores the users' sign-in credentials. When disabled, the user is always sees the prompt to sign into the Expressway server for Mobile and Remote Access (MRA). If you want to make it easier for users to log in, you enable this field so that the Expressway login credentials are persistent. The user then only has to enter their login credentials the first time. Any time after that (when the phone is powered on off-premises), the login information is prepopulated on the Sign-in screen. For more information, see the Configure User Credentials Persistent for Expressway Sign-In, on page 119.

Field Name	Field Type Or Choices	Default	Description
Customer support upload URL	String, up to 256 characters		Provides the URL for the Problem Report Tool (PRT). If you deploy devices with Mobile and Remote Access through Expressway, you must also add the PRT server address to the HTTP Server Allow list on the Expressway server. For more information, see the Configure User Credentials Persistent for Expressway Sign-In, on page 119.
Disable TLS Ciphers	See Disable Transport Layer Security Ciphers, on page 108.	None	Disables the selected TLS cipher. Disable more than one cipher suite by selecting and holding the **Ctrl** key on your computer keyboard.
Dedicate one line for Call Park	Disabled Enabled	Enabled	Controls whether a parked call occupies one line or not. For more information, see the Cisco Unified Communications Manager documentation.

Related Topics

Configure User Credentials Persistent for Expressway Sign-In, on page 119

Disable Transport Layer Security Ciphers

You can disable Transport Layer Security (TLS) ciphers with the **Disable TLS Ciphers** parameter. This allows you to tailor your security for known vulnerabilities, and to align your network with your company's policies for ciphers.

None is the default setting.

Disable more than one cipher suite by selecting and holding the **Ctrl** key on your computer keyboard. If you select all of the phone ciphers, then phone TLS service is impacted. Your choices are:

- None
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

For more information about phone security, see *Cisco IP Phone 7800 and 8800 Series Security Overview White Paper* (https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/white-paper-listing.html).

Schedule Power Save for Cisco IP Phone

To conserve power and ensure the longevity of the phone screen display, you can set the display to turn off when it is not needed.

You can configure settings in Cisco Unified Communications Manager Administration to turn off the display at a designated time on some days and all day on other days. For example, you may choose to turn off the display after business hours on weekdays and all day on Saturdays and Sundays.

You can take any of these actions to turn on the display any time it is off:

- Press any button on the phone.

  The phone takes the action designated by that button in addition to turning on the display.
- Lift the handset.

When you turn the display on, it remains on until the phone has remained idle for a designated length of time, then it turns off automatically.

Procedure

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

Step 2 Locate the phone that you need to set up.

Step 3 Navigate to the Product Specific Configuration area and set the following fields:

- Days Display Not Active
- Display On Time
- Display On Duration
- Display Idle Timeout

Table 19: PowerSave Configuration Fields

Field	Description
Days Display Not Active	Days that the display does not turn on automatically at the time specified in the Display On Time field. Choose the day or days from the drop-down list. To choose more than one day, Ctrl-click each day that you want.

Field	Description
Display On Time	Time each day that the display turns on automatically (except on the days specified in the Days Display Not Active field). Enter the time in this field in 24-hour format, where 0:00 is midnight. For example, to automatically turn the display on at 07:00a.m., (0700), enter **07:00**. To turn the display on at 02:00p.m. (1400), enter **14:00**. If this field is blank, the display will automatically turn on at 0:00.
Display On Duration	Length of time that the display remains on after turning on at the time specified in the Display On Time field. Enter the value in this field in the format *hours:minutes*. For example, to keep the display on for 4 hours and 30 minutes after it turns on automatically, enter **04:30**. If this field is blank, the phone will turn off at the end of the day (0:00). **Note** If Display On Time is 0:00 and the display on duration is blank (or 24:00), the display will remain on continuously.
Display Idle Timeout	Length of time that the phone is idle before the display turns off. Applies only when the display was off as scheduled and was turned on by a user (by pressing a button on the phone or lifting the handset). Enter the value in this field in the format *hours:minutes*. For example, to turn the display off when the phone is idle for 1 hour and 30 minutes after a user turns the display on, enter **01:30**. The default value is 01:00.

Step 4 Select **Save**.

Step 5 Select **Apply Config**.

Step 6 Restart the phone.

Schedule EnergyWise on Cisco IP Phone

To reduce power consumption, configure the phone to sleep (power down) and wake (power up) if your system includes an EnergyWise controller.

You configure settings in Cisco Unified Communications Manager Administration to enable EnergyWise and configure sleep and wake times. These parameters are closely tied to the phone display configuration parameters.

When EnergyWise is enabled and a sleep time is set, the phone sends a request to the switch to wake it up at the configured time. The switch returns either an acceptance or a rejection of the request. If the switch rejects the request or if the switch does not reply, the phone does not power down. If the switch accepts the request, the idle phone goes to sleep, thus reducing the power consumption to a predetermined level. A phone that is not idle sets an idle timer and goes to sleep after the idle timer expires.

To wake up the phone, press Select. At the scheduled wake time, the system restores power to the phone, waking it up.

Procedure

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

Step 2 Locate the phone that you need to set up.

Step 3 Navigate to the Product Specific Configuration area and set the following fields.

- Enable Power Save Plus
- Phone On Time
- Phone Off Time
- Phone Off Idle Timeout
- Enable Audible Alert
- EnergyWise Domain
- EnergyWise Secret
- Allow EnergyWise Overrides

Table 20: EnergyWise Configuration Fields

Field	Description
Enable Power Save Plus	Selects the schedule of days for which the phone powers off. Select multiple days by pressing and holding the Control key while clicking on the days for the schedule. By default, no days are selected. When Enable Power Save Plus is checked, you receive a message that warns about emergency (e911) concerns. **Caution** While Power Save Plus Mode (the "Mode") is in effect, endpoints that are configured for the mode are disabled for emergency calling and from receiving inbound calls. By selecting this mode, you agree to the following: (i) You take full responsibility for providing alternate methods for emergency calling and receiving calls while the mode is in effect; (ii) Cisco has no liability in connection with your selection of the mode and all liability in connection with enabling the mode is your responsibility; and (iii) You fully inform users of the effects of the mode on calls, calling and otherwise. **Note** To disable Power Save Plus, you must uncheck the Allow EnergyWise Overrides check box. If the Allow EnergyWise Overrides remains checked but no days are selected in the Enable Power Save Plus field, Power Save Plus is not disabled.

Field	Description
Phone On Time	Determines when the phone automatically turns on for the days that are in the Enable Power Save Plus field. Enter the time in this field in 24-hour format, where 00:00 is midnight. For example, to automatically power up the phone at 07:00 a.m. (0700), enter 07:00. To power up the phone at 02:00 p.m. (1400), enter 14:00. The default value is blank, which means 00:00. **Note** The Phone On Time must be at least 20 minutes later than the Phone Off Time. For example, if the Phone Off Time is 07:00, the Phone On Time must be no earlier than 07:20.
Phone Off Time	The time of day that the phone powers down for the days that are selected in the Enable Power Save Plus field. If the Phone On Time and the Phone Off Time fields contain the same value, the phone does not power down. Enter the time in this field in 24-hour format, where 00:00 is midnight. For example, to automatically power down the phone at 7:00 a.m. (0700), enter 7:00. To power down the phone at 2:00 p.m. (1400), enter 14:00. The default value is blank, which means 00:00. **Note** The Phone On Time must be at least 20 minutes later than the Phone Off Time. For example, if the Phone Off Time is 7:00, the Phone On Time must be no earlier than 7:20.
Phone Off Idle Timeout	The length of time that the phone must be idle before the phone powers down. The timeout occurs under the following conditions: • When the phone was in Power Save Plus mode, as scheduled, and was taken out of Power Save Plus mode because the phone user pressed the **Select** key. • When the phone is repowered by the attached switch. • When the Phone Off Time is reached but the phone is in use. The range of the field is 20 to 1440 minutes. The default value is 60 minutes.

Field	Description
Enable Audible Alert	When enabled, instructs the phone to play an audible alert starting 10 minutes before the time that the Phone Off Time field specifies. The audible alert uses the phone ringtone, which briefly plays at specific times during the 10-minute alerting period. The alerting ringtone plays at the user-designated volume level. The audible alert schedule is: • At 10 minutes before power down, play the ringtone four times. • At 7 minutes before power down, play the ringtone four times. • At 4 minutes before power down, play the ringtone four times. • At 30 seconds before power down, play the ringtone 15 times or until the phone powers off. This check box applies only if the Enable Power Save Plus list box has one or more days selected.
EnergyWise Domain	The EnergyWise domain that the phone is in. The maximum length of this field is 127 characters.
EnergyWise Secret	The security secret password that is used to communicate with the endpoints in the EnergyWise domain. The maximum length of this field is 127 characters.
Allow EnergyWise Overrides	This check box determines whether you allow the EnergyWise domain controller policy to send power level updates to the phones. The following conditions apply: • One or more days must be selected in the Enable Power Save Plus field. • The settings in Cisco Unified Communications Manager Administration take effect on schedule even if EnergyWise sends an override. For example, assuming the Phone Off Time is set to 22:00 (10:00 p.m.), the value in the Phone On Time field is 06:00 (6:00 a.m.), and the Enable Power Save Plus has one or more days selected. • If EnergyWise directs the phone to turn off at 20:00 (8:00 p.m.), that directive remains in effect (assuming no phone user intervention occurs) until the configured Phone On Time at 6:00 a.m. • At 6:00 a.m., the phone turns on and resumes receiving the power level changes from the settings in Unified Communications Manager Administration. • To change the power level on the phone again, EnergyWise must reissue a new power level change command. **Note** To disable Power Save Plus, you must uncheck the Allow EnergyWise Overrides check box. If the Allow EnergyWise Overrides remains checked but no days are selected in the Enable Power Save Plus field, Power Save Plus is not disabled.

Step 4 Select **Save**.

Step 5 Select **Apply Config**.

Step 6 Restart the phone.

Set Up Do Not Disturb

When Do Not Disturb (DND) is turned on, the header on the conference phone screen is red.

For more information, see the Do Not Disturb information in the documentation for your particular Cisco Unified Communications Manager release.

Procedure

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

Step 2 Locate the phone to be configured.

Step 3 Set the following parameters.

- Do Not Disturb: This check box allows you to enable DND on the phone.
- DND Option: Ring Off, Call Reject, or Use Common Phone Profile Setting.
- DND Incoming Call Alert: Choose the type of alert, if any, to play on a phone for incoming calls when DND is active.

Note This parameter is located on in the Common Phone Profile window and the Phone Configuration window. The Phone Configuration window value takes precedence.

Step 4 Select **Save**.

Related Topics

Cisco Unified Communications Manager Documentation, on page 14

Set Up Call Forward Notification

You can control the call forward settings.

Procedure

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

Step 2 Locate the phone to be set up.

Step 3 Configure the Call Forward Notification fields.

Field	Description
Caller Name	When this check box is checked, the caller name displays in the notification window. By default, this check box is checked.

Field	Description
Caller Number	When this check box is checked, the caller number displays in the notification window. By default, this check box is not checked.
Redirected Number	When this check box is checked, the information about the caller who last forwarded the call displays in the notification window. Example: If Caller A calls B, but B has forwarded all calls to C and C has forwarded all calls to D, the notification box that D sees contains the phone information for caller C. By default, this check box is not checked.
Dialed Number	When this check box is checked, the information about the original recipient of the call displays in the notification window. Example: If Caller A calls B, but B has forwarded all calls to C and C has forwarded all calls to D, then the notification box that D sees contains the phone information for caller B. By default, this check box is checked.

Step 4 Select **Save**.

UCR 2008 Setup

The parameters that support UCR 2008 reside in Cisco Unified Communications Manager Administration. The following table describes the parameters and indicates the path to change the setting.

Table 21: UCR 2008 Parameter Location

Parameter	Administration Path
FIPS Mode	**Device** > **Device Settings** > **Common Phone Profile**
	System > **Enterprise Phone Configuration**
	Device > **Phones**
SSH Access	**Device** > **Phone**
	Device > **Device Settings** > **Common Phone Profile**
Web Access	**Device** > **Phone**
	System > **Enterprise Phone Configuration**
	Device > **Device Settings** > **Common Phone Profile**
System > **Enterprise Phone Configuration**	

Parameter	Administration Path
IP Addressing Mode	**Device** > **Device Settings** > **Common Device Configuration**
IP Addressing Mode Preference for Signaling	**Device** > **Device Settings** > **Common Device Configuration**

Set Up UCR 2008 in Common Device Configuration

Use this procedure to set the following UCR 2008 parameters:

- IP Addressing Mode
- IP Addressing Mode Preference for Signaling

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Device** > **Device Settings** > **Common Device Configuration**.

Step 2 Set the IP Addressing Mode parameter.

Step 3 Set the IP Addressing Mode Preference for Signaling parameter.

Step 4 Select **Save**.

Set Up UCR 2008 in Common Phone Profile

Use this procedure to set the following UCR 2008 parameters:

- FIPS Mode
- SSH Access
- Web Access

Procedure

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

Step 2 Set the FIPS Mode parameter to **Enabled**.

Step 3 Set the SSH Access parameter to **Disabled**.

Step 4 Set the Web Access parameter to **Disabled**.

Step 5 Set the 80-bit SRTCP parameter to **Enabled**.

Step 6 Select **Save**.

Set Up UCR 2008 in Enterprise Phone Configuration

Use this procedure to set the following UCR 2008 parameters:

- FIPS Mode
- Web Access

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **System** > **Enterprise Phone Configuration**.

Step 2 Set the FIPS Mode parameter to **Enabled**.

Step 3 Set the Web Access parameter to **Disabled**.

Step 4 Select **Save**.

Set Up UCR 2008 in Phone

Use this procedure to set the following UCR 2008 parameters:

- FIPS Mode
- SSH Access
- Web Access

Procedure

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

Step 2 Set the SSH Access parameter to **Disabled**.

Step 3 Set the FIPS Mode parameter to **Enabled**.

Step 4 Set the Web Access parameter to **Disabled**.

Step 5 Select **Save**.

Mobile and Remote Access Through Expressway

Mobile and Remote Access Through Expressway(MRA) lets remote workers easily and securely connect into the corporate network without using a virtual private network (VPN) client tunnel. Expressway uses Transport Layer Security (TLS) to secure network traffic. For a phone to authenticate an Expressway certificate and establish a TLS session, a public Certificate Authority that the phone firmware trusts must sign the Expressway certificate. It is not possible to install or trust other CA certificates on phones for authenticating an Expressway certificate.

The list of CA certificates embedded in the phone firmware is available at http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-technical-reference-list.html.

Mobile and Remote Access Through Expressway (MRA)works with Cisco Expressway. You must be familiar with the Cisco Expressway documentation, including the *Cisco Expressway Administrator Guide* and the *Cisco Expressway Basic Configuration Deployment Guide*. Cisco Expressway documentation is available at http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/tsd-products-support-series-home.html.

Only the IPv4 protocol is supported for Mobile and Remote Access Through Expressway users.

For additional information about working with Mobile and Remote Access Through Expressway, see:

- *Cisco Preferred Architecture for Enterprise Collaboration, Design Overview*
- *Cisco Preferred Architecture for Enterprise Collaboration, CVD*
- *Unified Communications Mobile and Remote Access via Cisco VCS Deployment Guide*
- *Cisco TelePresence Video Communication Server (VCS), Configuration Guides*
- *Mobile and Remote Access Through Cisco Expressway Deployment Guide*

During the phone registration process, the phone synchronizes the displayed date and time with the Network Time Protocol (NTP) server. With MRA, the DHCP option 42 tag is used to locate the IP addresses of the NTP servers designated for time and date synchronization. If the DHCP option 42 tag is not found in the configuration information, the phone looks for the 0.tandberg.pool.ntp.org tag to identify the NTP servers.

After registration, the phone uses information from the SIP message to synchronize the displayed date and time unless an NTP server is configured in the Cisco Unified Communications Manager phone configuration.

Note If the phone security profile for any of your phones has TFTP Encrypted Config checked, you cannot use the phone with Mobile and Remote Access. The MRA solution does not support device interaction with Certificate Authority Proxy Function (CAPF).

SIP OAuth mode is supported for MRA. This mode allows you to use OAuth access tokens for authentication in secure environments.

Note For SIP OAuth in Mobile and Remote Access (MRA) mode, use only Activation Code Onboarding with Mobile and Remote Access when you deploy the phone. Activation with a username and password is not supported.

SIP OAuth mode requires Expressway x14.0(1) and later, or Cisco Unified Communications Manager 14.0(1) and later.

For additional information on SIP OAuth mode see *Feature Configuration Guide for Cisco Unified Communications Manager*, Release 14.0(1) or later.

Deployment Scenarios

The following table shows various deployment scenarios for Mobile and Remote Access Through Expressway.

Scenario	Actions
On-premises user logs in to the enterprise network, after deploying Mobile and Remote Access Through Expressway.	The enterprise network is detected, and the phone registers with Cisco Unified Communications Manager as it would normally.

Scenario	Actions
Off-premises user logs in to the enterprise network with Mobile and Remote Access Through Expressway.	The phone detects that it is in off-premises mode, the Mobile and Remote Access Through Expressway Sign-In window appears, and the user connects to the corporate network. Users must have a valid service name, username, and password to connect to the network. Users must also reset the service mode to clear the Alternate TFTP setting before they can access the company network. This clears the Alternate TFTP Server setting so the phone detects the off-premises network. If a phone is being deployed out of the box, users may skip the reset Network Settings requirement. If users have DHCP option 150 or option 66 enabled on their network router, they may not be able to sign in to the corporate network. Users should disable these DHCP settings or configure their static IP address directly.

Configure User Credentials Persistent for Expressway Sign-In

When a user signs in to the network with Mobile and Remote Access Through Expressway, the user is prompted for a service domain, username, and password. If you enable the User Credentials Persistent for Expressway Sign-In parameter, user login credentials are stored so that they do not need to reenter this information. This parameter is disabled by default.

You can set up credentials to persist for a single phone, a group of phones, or all phones.

Related Topics

Phone Feature Configuration, on page 95
Product Specific Configuration, on page 97

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.

If the PRT upload fails, you can access the PRT file for the phone from the URL **`http://<phone-ip-address>/FS/<prt-file-name>`**. This URL is displayed on the phone in the following cases:

- If the phone is in the factory default state. The URL is active for 1 hour. After 1 hour, the user should try to submit the phone logs again.
- If the phone has downloaded a configuration file and the call control system allows web access to the phone.

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

If you are deploying devices with Mobile and Remote Access through Expressway, you must also add the PRT server address to the HTTP Server Allow list on the Expressway server.

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.");
}

?>
```

Note The phones only support HTTP URLs.

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.

Set the Label for a Line

You can set up a phone to display a text label instead of the directory number. Use this label to identify the line by name or function. For example, if your user shares lines on the phone, you could identify the line with the name of the person that shares the line.

When adding a label to a key expansion module, only the first 25 characters are displayed on a line.

Procedure

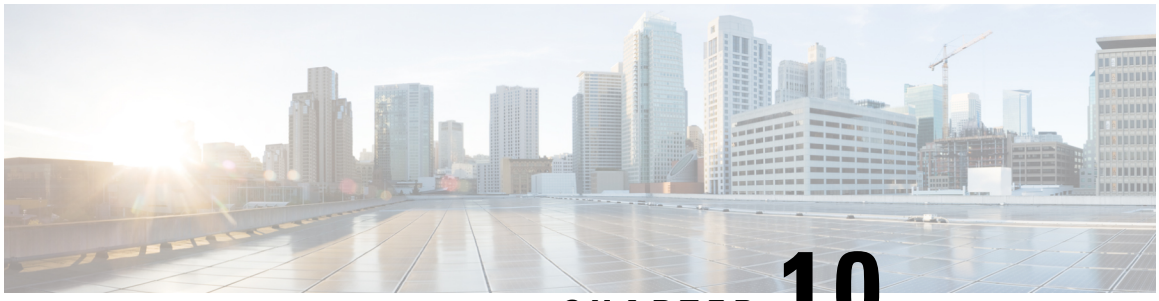
Step 1 In Cisco Unified Communications Manager Administration, select **Device** > **Phone**.

Step 2 Locate the phone to be configured.

Step 3 Locate the line instance and set the Line Text Label field.

Step 4 (Optional) If the label needs to be applied to other devices that share the line, check the Update Shared Device Settings check box and click **Propagate Selected**.

Step 5 Select **Save**.



CHAPTER 10

Corporate and Personal Directory

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.

Related Topics

Cisco Unified Communications Manager Documentation, on page 14

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:

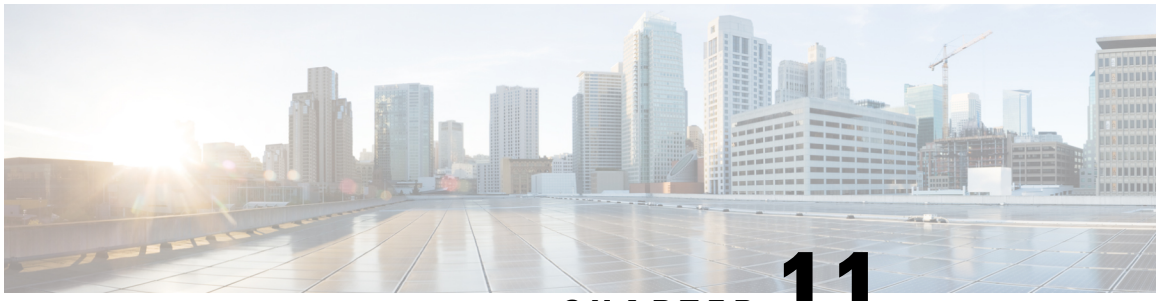
- From a web browser—Users can access the PAB and Speed Dials features from the Cisco Unified Communications Self Care Portal.

- From the CiscoIP 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.

PART IV

Cisco IP Conference Phone Troubleshooting



CHAPTER 11

Monitoring Phone Systems

Monitoring Phone Systems Overview

You can view a variety of information about the phone using the phone status menu on the phone and the phone web pages. This information includes:

- Device information
- Network setup information
- Network statistics
- Device logs
- Streaming statistics

This chapter describes the information that you can obtain from the phone web page. You can use this information to remotely monitor the operation of a phone and to assist with troubleshooting.

Related Topics

Phone Troubleshooting, on page 153

Cisco IP Phone Status

The following sections describes how to view model information, status messages, and network statistics on the Cisco IP Phone.

- Model Information: Displays hardware and software information about the phone.
- Status menu: Provides access to screens that display the status messages, network statistics, and statistics for the current call.

You can use the information that displays on these screens to monitor the operation of a phone and to assist with troubleshooting.

You can also obtain much of this information, and obtain other related information, remotely through the phone web page.

Display the Phone Information Window

Procedure

Step 1 Press **Settings** > **System information**.

Step 2 To exit the menu, press **Exit**.

Display the Status Menu

Procedure

Step 1 Press **Settings** > **Status**.

Step 2 To exit the menu, press **Exit**.

Display the Status Messages Window

Procedure

Step 1 Press **Settings** > **Status** > **Status Messages**.

Step 2 To exit the menu, press **Exit**.

Status Messages Fields

The following table describes the status messages that display on the Status Messages screen of the phone.

Table 22: Status Messages on the Cisco IP Phone

Message	Description	Possible Explanation and Action
Could not acquire an IP address from DHCP	The phone has not previously obtained an IP address from a DHCP Server. This can occur when you perform an out of box or factory reset.	Confirm that the DHCP server is availab is available for the phone.
TFTP Size Error	The configuration file is too large for file system on the phone.	Power cycle the phone.

Message	Description	Possible Explanation and Action
ROM Checksum Error	Downloaded software file is corrupted.	Obtain a new copy of the phone firm TFTPPath directory. You should on directory when the TFTP server softw the files may be corrupted.
Duplicate IP	Another device is using the IP address that is assigned to the phone.	If the phone has a static IP address, assigned a duplicate IP address. If you are using DHCP, check the D
Erasing CTL and ITL files	Erasing CTL or ITL file.	None. This message is informationa
Error Updating Locale	One or more localization files could not be found in the TFTP Path directory or were not valid. The locale was not changed.	From Cisco Unified Operating Syst that the following files are located v TFTP File Management: • Located in subdirectory with sa • tones.xml • Located in subdirectory with s • glyphs.xml • dictionary.xml • kate.xml
File not found <Cfg File>	The name-based and default configuration file was not found on the TFTP Server.	The configuration file for a phone i added to the Cisco Unified Commun If the phone does not exist in the Cis Manager database, the TFTP server **`Not Found`** response. • Phone is not registered with Cis Manager. You must manually add the ph Communications Manager if y to autoregister. • If you are using DHCP, verify pointing to the correct TFTP s • If you are using static IP addre the TFTP server.
File Not Found <CTLFile.tlv>	This message displays on the phone when the Cisco Unified Communications Manager cluster is not in secure mode.	No impact; the phone can still regis Communications Manager.
IP Address Released	The phone is configured to release the IP address.	The phone remains idle until it is po the DHCP address.

Message	Description	Possible Explanation and Action
IPv4 DHCP Timeout	IPv4 DHCP server did not respond.	Network is busy: The errors should res the network load reduces. No network connectivity between the I the phone: Verify the network connecti IPv4 DHCP server is down: Check conf server. Errors persist: Consider assigning a sta
IPv6 DHCP Timeout	IPv6 DHCP server did not respond.	Network is busy - The errors should re the network load reduces. No network connectivity between the I the phone: Verify the network connecti IPv6 DHCP server is down: Check conf server. Errors persist: Consider assigning a sta
IPv4 DNS Timeout	IPv4 DNS server did not respond.	Network is busy: The errors should res the network load reduces. No network connectivity between the I phone: Verify the network connections IPv4 DNS server is down: Check config server.
IPv6 DNS Timeout	IPv6 DNS server did not respond.	Network is busy: The errors should res the network load reduces. No network connectivity between the I phone: Verify the network connections IPv6 DNS server is down: Check config server.
DNS unknown IPv4 Host	IPv4 DNS could not resolve the name of the TFTP server or Cisco Unified Communications Manager.	Verify that the host names of the TFTP Communications Manager are configure Consider using IPv4 addresses rather th
DNS unknown IPv6 Host	IPv6 DNS could not resolve the name of the TFTP server or Cisco Unified Communications Manager.	Verify that the host names of the TFTP Communications Manager are configure Consider using IPv6 addresses rather th
Load Rejected HC	The application that was downloaded is not compatible with the phone hardware.	Occurs if you attempt to install a versio phone that did not support hardware ch Check the load ID that is assigned to th Unified Communications Manager, cho Reenter the load that displays on the ph

Message	Description	Possible Explanation and Action
No Default Router	DHCP or static configuration did not specify a default router.	If the phone has a static IP address, is configured. If you are using DHCP, the DHCP default router. Check the DHCP ser
No IPv4 DNS Server	A name was specified but DHCP or static IP configuration did not specify a IPv4 DNS server address.	If the phone has a static IP address, server is configured. If you are using DHCP, the DHCP IPv4 DNS server. Check the DHCP
No IPv6 DNS Server	A name was specified but DHCP or static IP configuration did not specify a IPv6 DNS server address.	If the phone has a static IP address, server is configured. If you are using DHCP, the DHCP IPv6 DNS server. Check the DHCP
No Trust List Installed	The CTL file or the ITL file is not installed on the phone.	The trust list is not configured on th Communications Manager, which d default. The trust list is not configured. For more information about trust lis for your particular Cisco Unified C release.
Phone failed to register. Cert key size is not FIPS compliant.	FIPS requires that the RSA server certificate is 2048 bits or greater.	Update the certificate.
Restart requested by Cisco Unified Communications Manager	The phone is restarting due to a request from Cisco Unified Communications Manager.	Configuration changes were likely Unified Communications Manager, pressed so that the changes take eff
TFTP Access Error	TFTP server is pointing to a directory that does not exist.	If you are using DHCP, verify that t to the correct TFTP server. If you are using static IP addresses, c server.
TFTP Error	The phone does not recognize an error code that the TFTP server provided.	Contact Cisco TAC.
TFTP Timeout	TFTP server did not respond.	Network is busy: The errors should the network load reduces. No network connectivity between the Verify the network connections. TFTP server is down: Check config
Timed Out	Supplicant attempted 802.1X transaction but timed out to due the absence of an authenticator.	Authentication typically times out i on the switch.

Message	Description	Possible Explanation and Action
Trust List Update Failed	Update of the CTL and ITL files failed.	Phone has CTL and ITL files installed a new CTL and ITL files. Possible reasons for failure: • Network failure occurred. • TFTP server was down. • The new security token that was u the TFTP certificate that was used introduced, but are not available i ITL files in the phone. • Internal phone failure occurred. Possible solutions: • Check network connectivity. • Check whether the TFTP server is normally. • If the Transactional Vsam Service supported on Cisco Unified Comm check whether the TVS server is a normally. • Verify whether the security token valid. Manually delete the CTL and ITL files solutions fail; reset the phone. For more information about trust lists, for your particular Cisco Unified Comm release.
Trust List Updated	The CTL file, the ITL file, or both files are updated.	None. This message is informational o For more information about trust lists, for your particular Cisco Unified Comm release.
Version Error	The name of the phone load file is incorrect.	Make sure that the phone load file has
XmlDefault.cnf.xml, or .cnf.xml corresponding to the phone device name	Name of the configuration file.	None. This message indicates the name for the phone.

Related Topics

Cisco Unified Communications Manager Documentation, on page 14

Display the Network Statistics Window

Procedure

Step 1 Press **Settings** > **Status** > **Network Statistics**.

Step 2 To exit the menu, press **Exit**,

Network Statistics Fields

The following table describes the information in the Network Statistics screen.

Table 23: Network Statistics Fields

Item	Description
Tx Frames	Number of packets sent by the phone
Tx broadcast	Number of broadcast packets sent by the phone
Tx unicast	Total number of unicast packets transmitted by the phone
Rx Frames	Number of packets received by the phone
Rx broadcast	Number of broadcast packets received by the phone
Rx unicast	Total number of unicast packets received by the phone
CDP Neighbor Device ID	Identifier of a device connected to this port discovered by CDP protocol.
CDP Neighbor IP Address	Identifier of a device connected to this port discovered by CDP protocol using IP.
CDP Neighbor Port	Identifier of a device connected to this port discovered by CDP protocol.
Restart Cause: One of these values: • Hardware Reset (Power-on reset) • Software Reset (memory controller also reset) • Software Reset (memory controller not reset) • Watchdog Reset • Initialized • Unknown	Cause of the last reset of the phone
Port 1	Link state and connection of the network port (for example, `100 Full` means that the PC port is in a link-up state and has auto-negotiated a full-duplex, 100-Mbps connection)

Item	Description
IPv4	Information on the DHCP status. This includes the following states: • CDP BOUND • CDP INIT • DHCP BOUND • DHCP DISABLED • DHCP INIT • DHCP INVALID • DHCP REBINDING • DHCP REBOOT • DHCP RENEWING • DHCP REQUESTING • DHCP RESYNC • DHCP UNRECOGNIZED • DHCP WAITING COLDBOOT TIMEOUT • DISABLED DUPLICATE IP • SET DHCP COLDBOOT • SET DHCP DISABLED • SET DHCP FAST

Item	Description
IPv6	Information on the DHCP status. This includes the following states: • CDP INIT • DHCP6 BOUND • DHCP6 DISABLED • DHCP6 RENEW • DHCP6 REBIND • DHCP6 INIT • DHCP6 SOLICIT • DHCP6 REQUEST • DHCP6 RELEASING • DHCP6 RELEASED • DHCP6 DISABLING • DHCP6 DECLINING • DHCP6 DECLINED • DHCP6 INFOREQ • DHCP6 INFOREQ DONE • DHCP6 INVALID • DISABLED DUPLICATE IPV6 • DHCP6 DECLINED DUPLICATE IP • ROUTER ADVERTISE • DHCP6 WAITING COLDBOOT TIMEOUT • DHCP6 TIMEOUT USING RESTORED VAL • DHCP6 TIMEOUT CANNOT RESTORE • IPV6 STACK TURNED OFF • ROUTER ADVERTISE • ROUTER ADVERTISE • UNRECOGNIZED MANAGED BY • ILLEGAL IPV6 STATE

Display the Call Statistics Window

Procedure

Step 1 Press **Settings** > **Status** > **Call Statistics**.

Step 2 To exit the menu, press **Exit**,

Call Statistics Fields

The following table describes the items on the Call Statistics screen.

Table 24: Call Statistics Items

Item	Description
Receiver Codec	Type of received voice stream (RTP streaming audio from codec): • G.729 • G.722 • G.722 AMR WB • G.711 mu-law • G.711 A-law • iLBC • OPUS
Sender Codec	Type of transmitted voice stream (RTP streaming audio from codec): • G.729 • G.722 • G.722 AMR WB • G.711 mu-law • G.711 A-law • iLBC • OPUS
Receiver Size	Size of voice packets, in milliseconds, in the receiving voice stream (RTP streaming audio).
Sender Size	Size of voice packets, in milliseconds, in the transmitting voice stream.

Item	Description
Rcvr Packets	Number of RTP voice packets that were received since voice stream opened. **Note** This number is not necessarily identical to the number of RTP voice packets that were received since the call began because the call might have been placed on hold.
Sender Packets	Number of RTP voice packets that were transmitted since voice stream opened. **Note** This number is not necessarily identical to the number of RTP voice packets that were transmitted since the call began because the call might have been placed on hold.
Avg Jitter	Estimated average RTP packet jitter (dynamic delay that a packet encounters when going through the network), in milliseconds, that was observed since the receiving voice stream opened.
Max Jitter	Maximum jitter, in milliseconds, that was observed since the receiving voice stream opened.
Receiver Discarded	Number of RTP packets in the receiving voice stream that were discarded (bad packets, too late, and so on). **Note** The phone discards payload type 19 comfort noise packets that Cisco Gateways generate, because they increment this counter.
Rcvr Lost Packets	Missing RTP packets (lost in transit).
Voice-Quality Metrics	
Cumulative Conceal Ratio	Total number of concealment frames divided by total number of speech frames that were 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	Estimate of the network latency, expressed in milliseconds. Represents a running average of the round-trip delay, measured when RTCP receiver report blocks are received.

Cisco IP Phone Web Page

Each Cisco IP Phone has a web page from which you can view a variety of information about the phone, including:

- Device Information: Displays device settings and related information for the phone.
- Network Setup: Displays network setup information and information about other phone settings.
- Network Statistics: Displays hyperlinks that provide information about network traffic.
- Device Logs: Displays hyperlinks that provide information that you can use for troubleshooting.
- Streaming Statistic: Displays hyperlinks to a variety of streaming statistics.

This section describes the information that you can obtain from the phone web page. You can use this information to remotely monitor the operation of a phone and to assist with troubleshooting.

You can also obtain much of this information directly from a phone.

Access the Phone Web Page

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 phone, press **Settings** > **System Information** and then scroll to the IPv4 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>

Device Information Web Page

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

To display the Device Information area, access the web page for the phone, and then click the **Device Information** hyperlink.

Table 25: Device Information Web Page Fields

Field	Description
Service mode	The service mode for the phone.
Service domain	The domain for the service.
Service state	The current state of the service.
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.
Phone DN	Directory number that is assigned to the phone.
App Load ID	Identifies the application load version.
Boot Load ID	Indicates the boot load version.
Version	Identifier of the firmware that is running on the phone.
Hardware Revision	Minor revision value of the phone hardware.
Serial Number	Unique serial number of the phone.
Model Number	Model number of the phone.
Message waiting	Indicates whether is a voice message is waiting on the primary line for this phone.
UDI	Displays the following Cisco Unique Device Identifier (UDI) information about the phone: • Hardware type • Phone model name • Product identifier • Version ID (VID)—Specifies the major hardware version number. • Serial number
Time	Time for the Date/Time Group to which the phone belongs. This information comes from Cisco Unified Communications Manager.
Time Zone	Time zone for the Date/Time Group to which the phone belongs. This information comes from Cisco Unified Communications Manager.
Date	Date for the Date/Time Group to which the phone belongs. This information comes from Cisco Unified Communications Manager.
System Free Memory	Amount of available system memory.
Java Heap Free Memory	Amount of free memory for the Java heap.

Field	Description
Java Pool Free Memory	Amount of free memory for the Java pool.
FIPS Mode Enabled	Indicates if the Federal Information processing Standard (FIPS) Mode is enabled.

Network Setup Web Page

The Network Setup area on a phone web page displays network setup information and information about other phone settings. The following table describes these items.

You can view and set many of these items from the Network Setup menu on the Cisco IP Phone.

To display the Network Setup area, access the web page for the phone, and then click the **Network Setup** hyperlink.

Table 26: Network Setup Area Items

Item	Description
MAC Address	Media Access Control (MAC) address of the phone.
Host Name	Host name that the DHCP server assigned to the phone.
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 phon the IP address.
BOOTP Server	Indicates whether the phone obtains the configuration from a Bootstrap Protocol (BootP) ser
DHCP	Indicates whether the phone uses DHCP.
IP Address	Internet Protocol (IP) address of the phone.
Subnet Mask	Subnet mask that the phone uses.
Default Router 1	Default router used that the phone uses.
DNS Server 1–3	Primary Domain Name System (DNS) server (DNS Server 1) and optional backup DNS serve Server 2 and 3) that the phone uses.
Alternate TFTP	Indicates whether the phone is using an alternative TFTP server.
TFTP Server 1	Primary Trivial File Transfer Protocol (TFTP) server used that the phone uses.
TFTP Server 2	Backup Trivial File Transfer Protocol (TFTP) server used that the phone uses.
DHCP Address Released	Indicates the setting of the DHCP Address Released option.
Operational VLAN ID	Operational Virtual Local Area Network (VLAN) that is configured on a Cisco Catalyst swit which the phone is a member.
Admin VLAN ID	Auxiliary VLAN in which the phone is a member.

Item	Description
Unified CM 1-5	Host names or IP addresses, in prioritized order, of the Cisco Unified Communications Mar with which the phone can register. An item can also show the IP address of an SRST rout capable of providing limited Cisco Unified Communications Manager functionality, if suc available. For an available server, an item shows the Cisco Unified Communications Manager serve and one of the following states: • Active: Cisco Unified Communications Manager server from which the phone is curren call-processing services • Standby: Cisco Unified Communications Manager server to which the phone switches server becomes unavailable • Blank: No current connection to this Cisco Unified Communications Manager serve An item may also include the Survivable Remote Site Telephony (SRST) designation, whi an SRST router capable of providing Cisco Unified Communications Manager functional limited feature set. This router assumes control of call processing if all other Cisco Unifie Communications Manager servers become unreachable. The SRST Cisco Unified Comm Manager always appears last in the list of servers, even if it is active. You configure the S address in the Device Pool section in Cisco Unified Communications Manager Configurat
Information URL	URL of the help text that appears on the phone.
Directories URL	URL of the server from which the phone obtains directory information.
Messages URL	URL of the server from which the phone obtains message services.
Services URL	URL of the server from which the phone obtains Cisco IP Phone services.
Idle URL	URL that the phone displays when the phone is idle for the time that the Idle URL Time fi and no menu is open.
Idle URL Time	Number of seconds that the phone is idle and no menu is open before the XML service th URL specifies activates.
Proxy Server URL	URL of proxy server, which makes HTTP requests to nonlocal host addresses on behalf o HTTP client and provides responses from the nonlocal host to the phone HTTP client.
Authentication URL	URL that the phone uses to validate requests that are made to the phone web server.
SW Port Setup	Speed and duplex of the switch port, where: • A = Auto Negotiate • 10H = 10-BaseT/half duplex • 10F = 10-BaseT/full duplex • 100H = 100-BaseT/half duplex • 100F = 100-BaseT/full duplex • 1000F = 1000-BaseT/full duplex • No Link= No connection to the switch port
User Locale	User locale that associates with the phone user. Identifies a set of detailed information to su including language, font, date and time formatting, and alphanumeric keyboard text infor

Item	Description
Network Locale	Network locale that associates with the phone user. Identifies a set of detailed information to the phone in a specific location, including definitions of the tones and cadences that the phon
User Locale Version	Version of the user locale that is loaded on the phone.
Network Locale Version	Version of the network locale that is loaded on the phone.
Speaker Enabled	Indicates whether the speakerphone is enabled on the phone.
Group Listen	Indicates whether the group listen feature is enabled on the phone. Group listen enables you using the handset and listen on the speaker at the same time.
GARP Enabled	Indicates whether the phone learns MAC addresses from Gratuitous ARP responses.
Auto Line Select Enabled	Indicates whether the phone shifts the call focus to incoming calls on all lines.
DSCP for Call Control	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 services.
Security Mode	Security mode that is set for the phone.
Web Access Enabled	Indicates whether web access is enabled (Yes) or disabled (No) for the phone.
SSH Access Enabled	Indicates whether the phone accepts or blocks the SSH connections.
CDP: SW Port	Indicates whether CDP support exists on the switch port (default is enabled). Enable CDP on the switch port for VLAN assignment for the phone, power negotiation, QoS management, and 802.1x security. Enable CDP on the switch port when the phone connects to a Cisco switch. When CDP is disabled in Cisco Unified Communications Manager, a warning is presented, i that CDP should be disabled on the switch port only if the phone connects to a non-Cisco sw The current PC and switch port CDP values are shown on the Settings menu.
LLDP-MED: SW Port	Indicates whether Link Layer Discovery Protocol Media Endpoint Discovery (LLDP-MED) is on the switch port.
LLDP Power Priority	Advertises the phone power priority to the switch, thus enabling the switch to appropriately p power to the phones. Settings include: • Unknown: This is the default value. • Low • High • Critical
LLDP Asset ID	Identifies the asset ID that is assigned to the phone for inventory management.
CTL File	Identifies the CTL file.

Item	Description
ITL File	The ITL file contains the initial trust list.
ITL Signature	Enhances security by using the secure hash algorithm (SHA-1) in the CTL and ITL files.
CAPF Server	The name of the CAPF server used by the phone.
TVS	The main component of Security by Default. Trust Verification Services (TVS) enables C IP Phones to authenticate application servers, such as EM services, directory, and MIDlet HTTPS establishment.
TFTP Server	The name of the TFTP Server used by the phone.
Automatic Port Synchronization	Synchronizes the ports to the lower speed which eliminates packet loss.
Switch Port Remote Configuration	Allows the administrator to configure the speed and function of the Cisco Desktop Collab Experience table port remotely by using Cisco Unified Communications Manager Admin
PC Port Remote Configuration	Indicates if remote port configuration of the speed and duplex mode for the PC port is ena disabled.
IP Addressing Mode	Displays the IP addressing mode that is available on the phone.
IP Preference Mode Control	Indicates the IP address version that the phone uses during signaling with Cisco Unified Com Manager when both IPv4 and IPv6 are both available on the phone.
IP Preference Mode For Media	Indicates that for media the device uses an IPv4 address to connect to the Cisco Unified Com Manager.
IPv6 Auto Configuration	Displays whether the auto configuration is enabled or disabled on the phone.
IPv6 DAD	Verifies the uniqueness of new unicast IPv6 addresses before the addresses are assigned t
IPv6 Accept Redirect Message	Indicates if the phone accepts the redirect messages from the same router that is used for th number.
IPv6 Reply Multicast Echo Request	Indicates that the phone sends an Echo Reply message in response to an Echo Request m to an IPv6 address.
IPv6 Load Server	Used to optimize installation time for phone firmware upgrades and off load the WAN by images locally, negating the need to traverse the WAN link for each phone's upgrade.
IPv6 Log Server	Indicates the IP address and port of the remote logging machine to which the phone sends lo
IPv6 CAPF Server	Common Name (from the Cisco Unified Communications Manager Certificate) of the CA the phone.
DHCPv6	Dynamic Host Configuration Protocol (DHCP) automatically assigns IPv6 address to dev you connect them to the network. Cisco Unified IP Phones enable DHCP by default.
IPv6 Address	Displays the current IPv6 address of the phone or allows the user to enter a new IPv6 add
IPv6 Prefix Length	Displays the current prefix length for the subnet or allows the user to enter a new prefix l

Item	Description
IPv6 Default Router 1	Displays the default router used by the phone or allows the user to enter a new IPv6 default r
IPv6 DNS Server 1	Displays the primary DNSv6 server used by the phone or allows the user to enter a new serv
IPv6 DNS Server 2	Displays the secondary DNSv6 server used by the phone or allows the user to set a new seco DNSv6 server.
IPv6 Alternate TFTP	Allows the user to enable the use of an alternate (secondary) IPv6 TFTP server.
IPv6 TFTP Server 1	Displays the primary IPv6 TFTP server used by the phone or allows the user to set a new prima server.
IPv6 TFTP Server 2	Displays the secondary IPv6 TFTP server used if the primary IPv6 TFTP server is unavailable the user to set a new secondary TFTP server.
IPv6 Address Released	Allows the user to release IPv6-related information.
Energywise Power Level	A measure of the energy consumed by devices in an EnergyWise network.
Energywise Domain	An administrative grouping of devices for the purpose of power monitoring and control.

Ethernet Information Web Page

The following table describes the contents of the Ethernet Information web page.

Table 27: Ethernet Information Items

Item	Description
Tx Frames	Total number of packets that the phone transmits.
Tx broadcast	Total number of broadcast packets that the phone transmits.
Tx multicast	Total number of multicast packets that the phone transmits.
Tx unicast	Total number of unicast packets that the phone transmits.
Rx Frames	Total number of packets received by the phone.
Rx broadcast	Total number of broadcast packets that the phone receives..
Rx multicast	Total number of multicast packets that the phone receives.
Rx unicast	Total number of unicast packets that the phone receives.
Rx PacketNoDes	Total number of shed packets that the no Direct Memory Access (DMA) descriptor causes.

Network Web Pages

The following table describes the information in the Network Area web pages.

Note When you click the **Network** link under Network statistics, the page is titled "Port Information".

Table 28: Network Area items

Item	Description
Rx totalPkt	Total number of packets that the phone received.
Rx multicast	Total number of multicast packets that the phone received.
Rx broadcast	Total number of broadcast packets that the phone received.
Rx unicast	Total number of unicast packets that the phone received.
Rx tokenDrop	Total number of packets that were dropped due to lack of resources (for example, FIFO overflow).
Tx totalGoodPkt	Total number of good packets (multicast, broadcast, and unicast) that the phone received.
Tx broadcast	Total number of broadcast packets that the phone transmitted.
Tx multicast	Total number of multicast packets that the phone transmitted.
LLDP FramesOutTotal	Total number of LLDP frames that the phone sent out.
LLDP AgeoutsTotal	Total number of LLDP frames that timed out in the cache.
LLDP FramesDiscardedTotal	Total number of LLDP frames that were discarded when any of the mandatory TLVs is missing, out of order, or contains out of range string length.
LLDP FramesInErrorsTotal	Total number of LLDP frames that were received with one or more detectable errors.
LLDP FramesInTotal	Total number of LLDP frames that the phone receives.
LLDP TLVDiscardedTotal	Total number of LLDP TLVs that are discarded.
LLDP TLVUnrecognizedTotal	Total number of LLDP TLVs that are not recognized on the phone.
CDP Neighbor Device ID	Identifier of a device connected to this port that CDP discovered.
CDP Neighbor IP Address	IP address of the neighbor device discovered that CDP discovered.
CDP Neighbor IPv6 Address	IPv6 address of the neighbor device discovered that CDP discovered.
CDP Neighbor Port	Neighbor device port to which the phone is connected that CDP discovered.
LLDP Neighbor Device ID	Identifier of a device connected to this port that LLDP discovered.
LLDP Neighbor IP Address	IP address of the neighbor device that LLDP discovered.

Item	Description
LLDP Neighbor IPv6 Address	IPv6 address of the neighbor device that CDP discovered.
LLDP Neighbor Port	Neighbor device port to which the phone connects that LLDP discovered.
Port Information	Speed and duplex information.

Console Logs, Core Dumps, Status Messages, and Debug Display Web Pages

Under the Device Logs heading, the Console Logs, Core Dumps, Status Messages, and Debug Display hyperlinks provide information that helps to monitor and troubleshoot the phone.

- Console Logs—Includes hyperlinks to individual log files. The console log files include debug and error messages that the phone received.
- Core Dumps—Includes hyperlinks to individual dump files. The core dump files include data from a phone crash.
- Status Messages—Displays the 10 most recent status messages that the phone has generated since it last powered up. You can also get this information from the Status Messages screen on the phone.
- Debug Display—Displays debug messages that might be useful to Cisco TAC if you require assistance with troubleshooting.

Streaming Statistics Web Page

A Cisco IP Phone can stream information to and from up to five devices simultaneously. A phone streams information when it is on a call or is running a service that sends or receives audio or data.

The Streaming statistics areas on a phone web page provide information about the streams.

To display a Streaming Statistics area, access the web page for the phone, and then click a **Stream** hyperlink.

The following table describes the items in the Streaming Statistics areas.

Table 29: Streaming Statistics Fields

Item	Description
Remote Address	IP address and UDP port of the destination of the stream.
Local Address	IP address and UPD port of the phone.
Start Time	Internal time stamp indicates when Cisco Unified Communications Manager requested t phone start transmitting packets.
Stream Status	Indication of whether streaming is active or not.
Host Name	Unique, fixed name that is automatically assigned to the phone based on the MAC addr
Sender Packets	Total number of RTP data packets that the phone transmitted since it started this conne The value is 0 if the connection is set to receive-only mode.

Item	Description
Sender Octets	Total number of payload octets that the phone transmitted in RTP data packets since this connection. The value is 0 if the connection is set to receive-only mode.
Sender Codec	Type of audio encoding that is for the transmitted stream.
Sender Reports Sent (see note)	Number of times the RTCP Sender Report has been sent.
Sender Report Time Sent (see note)	Internal time-stamp indication as to when the last RTCP Sender Report was sent.
Rcvr Lost Packets	Total number of RTP data packets that have been lost since data reception started on connection. Defined as the number of expected packets less the number of packets received, where the number of received packets includes any that are late or are dupl value displays as 0 if the connection was set to send-only mode.
Avg Jitter	Estimate of mean deviation of the RTP data packet interarrival time, measured in mi The value displays as 0 if the connection was set to send-only mode.
Receiver Codec	Type of audio encoding that is used for the received stream.
Receiver Reports Sent (see note)	Number of times the RTCP Receiver Reports have been sent.
Receiver Report Time Sent (see note)	Internal time-stamp indication as to when a RTCP Receiver Report was sent.
Rcvr Packets	Total number of RTP data packets that the phone has received since data reception s this connection. Includes packets that were received from different sources if this ca multicast call. The value displays as 0 if the connection was set to send-only mode.
Rcvr Octets	Total number of payload octets that the device received in RTP data packets since r started on the connection. Includes packets that were received from different sources is a multicast call. The value displays as 0 if the connection was set to send-only mo
Cumulative Conceal Ratio	Total number of concealment frames divided by total number of speech frames that we from the start of the voice stream.
Interval Conceal Ratio	Ratio of concealment frames to speech frames in the preceding 3-second interval of speech. If voice activity detection (VAD) is in use, a longer interval might be requir accumulate three seconds of active speech.
Max Conceal Ratio	Highest interval concealment ratio from the start of the voice stream.
Conceal Seconds	Number of seconds that have concealment events (lost frames) from the start of the vo (includes severely concealed seconds).
Severely Conceal Seconds	Number of seconds that have more than five percent concealment events (lost frames start of the voice stream.

Item	Description
Latency (see note)	Estimate of the network latency, expressed in milliseconds. Represents a running avera the round-trip delay, measured when RTCP receiver report blocks are received.
Max Jitter	Maximum value of instantaneous jitter, in milliseconds.
Sender Size	RTP packet size, in milliseconds, for the transmitted stream.
Sender Reports Received (see note)	Number of times RTCP Sender Reports have been received.
Sender Report Time Received (see note)	Most recent time when an RTCP Sender Report was received.
Receiver Size	RTP packet size, in milliseconds, for the received stream.
Receiver Discarded	RTP packets that were received from the network but were discarded from the jitter bu
Receiver Reports Received (see note)	Number of times RTCP Receiver Reports have been received.
Receiver Report Time Received (see note)	Most recent time when an RTCP Receiver Report was received.

Note When the RTP Control Protocol is disabled, no data generates for this field and thus displays as 0.

Request Information from the Phone in XML

For troubleshooting purposes, you can request information from the phone. The resulting information is in XML format. The following information is available:

- CallInfo is call session information for a specific line.
- LineInfo is line configuration information for the phone.
- ModeInfo is phone mode information.

Before you begin

Web access needs to be enabled to get the information.

The phone must be associated with a user.

Procedure

Step 1 For Call Info, enter the following URL in a browser: **http://<phone ip address>/CGI/Java/CallInfo<x>**

where

- <*phone ip address*> is the IP address of the phone
- <*x*> is the line number to obtain information about.

The command returns an XML document.

Step 2 For Line Info, enter the following URL in a browser: **http://<phone ip address>/CGI/Java/LineInfo**

where

- <*phone ip address*> is the IP address of the phone

The command returns an XML document.

Step 3 For Model Info, enter the following URL in a browser: **http://<phone ip address>/CGI/Java/ModeInfo**

where

- <*phone ip address*> is the IP address of the phone

The command returns an XML document.

Sample CallInfo Output

The following XML code is an example of the output from the CallInfo command.

```
<?xml version="1.0" encoding="UTF-8"?>
<CiscoIPPhoneCallLineInfo>
  <Prompt/>
  <Notify/>
  <Status/>
  <LineDirNum>1030</LineDirNum>
  <LineState>CONNECTED</LineState>
  <CiscoIPPhoneCallInfo>
     <CallState>CONNECTED</CallState>
     <CallType>INBOUND</CallType>
     <CallingPartyName/>
     <CallingPartyDirNum>9700</CallingPartyDirNum>
     <CalledPartyName/>
     <CalledPartyDirNum>1030</CalledPartyDirNum>
     <HuntPilotName/>
     <CallReference>30303060</CallReference>
     <CallDuration>12835</CallDuration>
     <CallStatus>null</CallStatus>
     <CallSecurity>UNAUTHENTICATED</CallSecurity>
     <CallPrecedence>ROUTINE</CallPrecedence>
     <FeatureList/>
```

```
   </CiscoIPPhoneCallInfo>
   <VisibleFeatureList>
     <Feature Position="1" Enabled="true" Label="End Call"/>
     <Feature Position="2" Enabled="true" Label="Show Detail"/>
   </VisibleFeatureList>
</CiscoIPPhoneCallLineInfo>
```

Sample LineInfo Output

The following XML code is an example of the output from the LineInfo command.

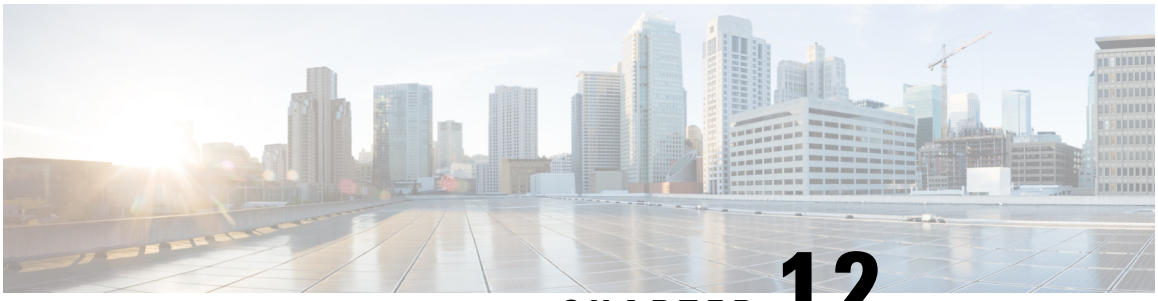
```
<CiscoIPPhoneLineInfo>
   <Prompt/>
   <Notify/>
   <Status>null</Status>
   <CiscoIPPhoneLines>
     <LineType>9</LineType>
     <lineDirNum>1028</lineDirNum>
     <MessageWaiting>NO</MessageWaiting>
     <RingerName>Chirp1</RingerName>
     <LineLabel/>
     <LineIconState>ONHOOK</LineIconState>
   </CiscoIPPhoneLines>
   <CiscoIPPhoneLines>
     <LineType>9</LineType>
     <lineDirNum>1029</lineDirNum>
     <MessageWaiting>NO</MessageWaiting>  <RingerName>Chirp1</RingerName>
     <LineLabel/>
     <LineIconState>ONHOOK</LineIconState>
   </CiscoIPPhoneLines>
   <CiscoIPPhoneLines>
     <LineType>9</LineType>
     <lineDirNum>1030</lineDirNum>
     <MessageWaiting>NO</MessageWaiting>
     <RingerName>Chirp1</RingerName>
     <LineLabel/>
     <LineIconState>CONNECTED</LineIconState>
   </CiscoIPPhoneLines>
   <CiscoIPPhoneLines>
     <LineType>2</LineType>
     <lineDirNum>9700</lineDirNum>
     <MessageWaiting>NO</MessageWaiting>
     <LineLabel>SD9700</LineLabel>
     <LineIconState>ON</LineIconState>
  </CiscoIPPhoneLines>
</CiscoIPPhoneLineInfo>
```

Sample ModeInfo Output

The following XML code is an example of the output from the ModeInfo command.

```
<?xml version="1.0" encoding="utf-8"?>
<CiscoIPPhoneModeInfo>
   <PlaneTitle>Applications</PlaneTitle>
   <PlaneFieldCount>12</PlaneFieldCount>
   <PlaneSoftKeyIndex>0</PlaneSoftKeyIndex>
   <PlaneSoftKeyMask>0</PlaneSoftKeyMask>
   <Prompt></Prompt>
   <Notify></Notify>
   <Status></Status>
```

```
   <CiscoIPPhoneFields>
      <FieldType>0</FieldType>
      <FieldAttr></FieldAttr>
      <fieldHelpIndex>0</fieldHelpIndex>
      <FieldName>Call History</FieldName>
      <FieldValue></FieldValue>
   </CiscoIPPhoneFields>
   <CiscoIPPhoneFields>
      <FieldType>0</FieldType>
      <FieldAttr></FieldAttr>
      <fieldHelpIndex>0</fieldHelpIndex>
      <FieldName>Preferences</FieldName>
      <FieldValue></FieldValue>
   </CiscoIPPhoneFields>
   ...
</CiscoIPPhoneModeInfo>
```



CHAPTER 12

Phone Troubleshooting

General Troubleshooting Information

The following table provides general troubleshooting information for the Cisco IP Phone.

Table 30: Cisco IP Phone Troubleshooting

Summary	Explanation
Prolonged broadcast storms cause IP phones to reset, or be unable to make or answer a call	A prolonged Layer 2 broadcast storm (lasting several minutes) on the v may cause IP phones to reset, lose an active call, or be unable to initiat call. Phones may not come up until a broadcast storm ends.
Moving a network connection from the phone to a workstation	If you power your phone through the network connection, you must be decide to unplug the network connection of the phone and plug the cable i computer. **Caution** The network card in the computer cannot receive power th network connection; if power comes through the connection, card can be destroyed. To protect a network card, wait 10 s longer after unplugging the cable from the phone before plu a computer. This delay gives the switch enough time to rec there is no longer a phone on the line and to stop providing the cable.

Summary	Explanation
Changing the telephone configuration	By default, the administrator password settings are locked to prevent users making changes that could impact their network connectivity. You must un administrator password settings before you can configure them. See Apply a Phone Password, on page 41 for details. **Note** If the administrator password is not set in common phone prof the user can modify the network settings.
Codec mismatch between the phone and another device	The RxType and the TxType statistics show the codec that is used for a con between this Cisco IP Phone and the other device. The values of these statisti match. If they do not, verify that the other device can handle the codec conv or that a transcoder is in place to handle the service. See Display the Call S Window, on page 136 for details.
Sound sample mismatch between the phone and another device	The RxSize and the TxSize statistics show the size of the voice packets tha in a conversation between this Cisco IP Phone and the other device. The va these statistics should match. See Display the Call Statistics Window, on p for details.
Loopback condition	A loopback condition can occur when the following conditions are met: • The SW Port Configuration option on the phone is set to 10 Half (10-B duplex). • The phone receives power from an external power supply. • The phone is powered down (the power supply is disconnected). In this case, the switch port on the phone can become disabled and the foll message appears in the switch console log: HALF_DUX_COLLISION_EXCEED_THRESHOLD To resolve this problem, reenable the port from the switch.

Startup Problems

After you install a phone into your network and add it to Cisco Unified Communications Manager, the phone should start up as described in the related topic below.

If the phone does not start up properly, see the following sections for troubleshooting information.

Related Topics

Verify the Phone Startup, on page 52

Cisco IP Phone Does Not Go Through the Normal Startup Process

Problem

When you connect a Cisco IP Phone to the network port, the phone does not go through the normal startup process as described in the related topic and the phone screen does not display information.

Cause

If the phone does not go through the startup process, the cause may be faulty cables, bad connections, network outages, lack of power, or the phone may not be functional.

Solution

To determine whether the phone is functional, use the following suggestions to eliminate other potential problems.

- Verify that the network port is functional:
  - Exchange the Ethernet cables with cables that you know are functional.
  - Disconnect a functioning Cisco IP Phone from another port and connect it to this network port to verify that the port is active.
  - Connect the Cisco IP Phone that does not start up to a different network port that is known to be good.
  - Connect the Cisco IP Phone that does not start up directly to the port on the switch, eliminating the patch panel connection in the office.
- Verify that the phone is receiving power:
  - If you are using external power, verify that the electrical outlet is functional.
  - If you are using in-line power, use the external power supply instead.
  - If you are using the external power supply, switch with a unit that you know to be functional.
- If the phone still does not start up properly, power up the phone from the backup software image.
- If the phone still does not start up properly, perform a factory reset of the phone.
- After you attempt these solutions, if the phone screen on the Cisco IP Phone does not display any characters after at least five minutes, contact a Cisco technical support representative for additional assistance.

Related Topics

Verify the Phone Startup, on page 52

Cisco IP Phone Does Not Register with Cisco Unified Communications Manager

If the phone proceeds past the first stage of the startup process (LED buttons flashing on and off) but continues to cycle through the messages that displays on the phone screen, the phone is not starting up properly. The phone cannot successfully start up unless it connects to the Ethernet network and it registers with a Cisco Unified Communications Manager server.

In addition, problems with security may prevent the phone from starting up properly. See Troubleshooting Procedures, on page 164 for more information.

Phone Displays Error Messages

Problem

Status messages display errors during startup.

Solution

While the phone cycles through the startup process, you can access status messages that might provide you with information about the cause of a problem. See the “Display Status Messages Window” section for instructions about accessing status messages and for a list of potential errors, their explanations, and their solutions.

Related Topics

Display the Status Messages Window, on page 128

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 settings may not be correct.

Solution

Check the TFTP settings.

Related Topics

Check TFTP Settings, on page 165

Phone Cannot Connect to Server

Problem

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

Solution

You should verify the IP addressing and routing settings on the phone. If you are using DHCP, the DHCP server should provide these values. If you have assigned a static IP address to the phone, you must enter these values manually.

Related Topics

Check DHCP Settings, on page 166

Phone Cannot Connect Using DNS

Problem

The DNS settings may be incorrect.

Solution

If you use DNS to access the TFTP server or Cisco Unified Communications Manager, you must ensure that you specify a DNS server.

Related Topics

Verify DNS Settings, on page 167

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 167.

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.

Related Topics

Create a New Phone Configuration File, on page 166

Cisco Unified Communications Manager Phone Registration

Problem

The phone is not registered with the Cisco Unified Communications Manager

Solution

A Cisco IP Phone can register with a Cisco Unified Communications Manager server only if the phone is added to the server or if autoregistration is enabled. Review the information and procedures in Phone Addition Methods, on page 60 to ensure that the phone is added to the Cisco Unified Communications Manager database.

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 Phone MAC Address, on page 59.

If the phone is already in the Cisco Unified Communications Manager database, the configuration file may be damaged. See Configuration File Corruption, on page 157 for assistance.

Cisco IP Phone Cannot Obtain IP Address

Problem

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

Solution

Ensure that the network or VLAN to which the phone connects has access to the DHCP server, and ensure that the switch port is enabled.

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 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 166

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 Cisco IP Phone received a command from Cisco Unified Communications Manager to reset by pressing **Settings** on the phone and choosing **Admin Settings** > **Status** > **Network Statistics**.

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

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

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 165.

Phone Does Not Power Up

Problem

The phone does not appear to be powered up.

Solution

In most cases, a phone restarts if it powers up by using external power but loses that connection and switches to PoE. Similarly, a phone may restart if it powers up by using PoE and then connects to an external power supply.

Phone Cannot Connect to LAN

Problem

The physical connection to the LAN may be broken.

Solution

Verify that the Ethernet connection to which the Cisco IP Phone connects is up. For example, check whether the particular port or switch to which the phone connects is down and that the switch is not rebooting. Also ensure that no cable breaks exist.

Cisco IP Phone Security Problems

The following sections provide troubleshooting information for the security features on the Cisco IP Phone. For information about the solutions for any of these issues, and for additional troubleshooting information about security, see *Cisco Unified Communications Manager Security Guide*.

CTL File Problems

The following sections describe troubleshooting problems with the CTL file.

Authentication Error, Phone Cannot Authenticate CTL File

Problem

A device authentication error occurs.

Cause

CTL file does not have a Cisco Unified Communications Manager certificate or has an incorrect certificate.

Solution

Install a correct certificate.

Phone Cannot Authenticate CTL File

Problem

Phone cannot authenticate the CTL file.

Cause

The security token that signed the updated CTL file does not exist in the CTL file on the phone.

Solution

Change the security token in the CTL file and install the new file on the phone.

CTL File Authenticates but Other Configuration Files Do Not Authenticate

Problem

Phone cannot authenticate any configuration files other than the CTL file.

Cause

A bad TFTP record exists, or the configuration file may not be signed by the corresponding certificate in the phone Trust List.

Solution

Check the TFTP record and the certificate in the Trust List.

ITL File Authenticates but Other Configuration Files Do Not Authenticate

Problem

Phone cannot authenticate any configuration files other than the ITL file.

Cause

The configuration file may not be signed by the corresponding certificate in the phone Trust List.

Solution

Re-sign the configuration file by using the correct certificate.

TFTP Authorization Fails

Problem

Phone reports TFTP authorization failure.

Cause

The TFTP address for the phone does not exist in the CTL file.

If you created a new CTL file with a new TFTP record, the existing CTL file on the phone may not contain a record for the new TFTP server.

Solution

Check the configuration of the TFTP address in the phone CTL file.

Phone Does Not Register

Problem

Phone does not register with Cisco Unified Communications Manager.

Cause

The CTL file does not contain the correct information for the Cisco Unified Communications Manager server.

Solution

Change the Cisco Unified Communications Manager server information in the CTL file.

Signed Configuration Files Are Not Requested

Problem

Phone does not request signed configuration files.

Cause

The CTL file does not contain any TFTP entries with certificates.

Solution

Configure TFTP entries with certificates in the CTL file.

Audio Problems

The following sections describe how to resolve audio problems.

No Speech Path

Problem

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

Solution

When at least one person in a call does not receive audio, IP connectivity between phones is not established. Check the configuration of routers and switches to ensure that IP connectivity is properly configured.

Choppy Speech

Problem

A user complains of choppy speech on a call.

Cause

There may be a mismatch in the jitter configuration.

Solution

Check the AvgJtr and the MaxJtr statistics. A large variance between these statistics might indicate a problem with jitter on the network or periodic high rates of network activity.

One Phone in Daisy Chain Mode Doesn't Work

Problem

In daisy chain mode, one of the conference phones does not work.

Solution

Check if the cables connected to the Smart Adapter are the correct ones. The two thicker cables connect the phones to the Smart Adapter. The thinner cable connects the Smart Adapter to the power adapter.

Related Topics

Daisy Chain Mode, on page 31
Install the Conference Phone in Daisy Chain Mode, on page 38

General Telephone Call Problems

The following sections help troubleshoot general telephone call problems.

Phone Call Cannot Be Established

Problem

A user complains about not being able to make a call.

Cause

The phone does not have a DHCP IP address, is unable to register to Cisco Unified Communications Manager. Phones with an LCD display show the message `Configuring IP` or `Registering`. Phones without an LCD display play the reorder tone (instead of dial tone) in the handset when the user attempts to make a call.

Solution

1. Verify the following:
   a. The Ethernet cable is attached.
   b. The Cisco CallManager service is running on the Cisco Unified Communications Manager server.
   c. Both phones are registered to the same Cisco Unified Communications Manager.
2. Audio server debug and capture logs are enabled for both phones. If needed, enable Java debug.

Phone Does Not Recognize DTMF Digits or Digits Are Delayed

Problem

The user complains that numbers are missed or delayed when the keypad is used.

Cause

Pressing the keys too quickly can result in missed or delayed digits.

Solution

Keys should not be pressed rapidly.

Troubleshooting Procedures

These procedures can be used to identify and correct problems.

Create a Phone Problem Report from Cisco Unified Communications Manager

You can generate a problem report for the phones from Cisco Unified Communications Manager. This action results in the same information that the Problem Report Tool (PRT) softkey generates on the phone.

The problem report contains information about the phone and the headsets.

Procedure

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

Step 2 Click **Find** and select one or more Cisco IP Phones.

Step 3 Click **Generate PRT for Selected** to collect PRT logs for the headsets used on the selected Cisco IP Phones.

Check TFTP Settings

Procedure

Step 1 Check the TFTP Server 1 field.

If you have assigned a static IP address to the phone, you must manually enter a setting for the TFTP Server 1 option.

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 2 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 3 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 scenarios.

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

Determine the Phone MAC Address, on page 59
Restart or Reset the Conference Phone, on page 171

Check DHCP Settings

Procedure

Step 1 On the phone, press **Settings**.

Step 2 Select **Admin Settings** > **Ethernet Setup** > **IPv4 Setup**.

Step 3 Check the DHCP server field.

If you have assigned a static IP address to the phone, you do not need to enter a value for the DHCP Server option. However, if you are using a DHCP server, this option must have a value. If no value is found, check your IP routing and VLAN configuration. See the *Troubleshooting Switch Port and Interface Problems* document, available at this URL:

https://www.cisco.com/en/US/customer/products/hw/switches/ps708/prod_tech_notes_list.html

Step 4 Check the IP Address, Subnet Mask, and Default Router fields.

If you assign a static IP address to the phone, you must manually enter settings for these options.

Step 5 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:

https://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a00800f0804.shtml

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.

Related Topics

Phone Addition Methods, on page 60
Cisco Unified Communications Manager Documentation, on page 14

Verify DNS Settings

Procedure

Step 1 On the phone, press **Settings**.

Step 2 Select **Admin Settings** > **Ethernet Setup** > **IPv4 Setup**

Step 3 Check that the DNS Server 1 field is set correctly.

Step 4 You should also verify that a CNAME entry was made in the DNS server for the TFTP server and for the Cisco Unified Communications Manager system.

You must also ensure that DNS is configured to do reverse lookups.

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.

Control Debug Information from Cisco Unified Communications Manager

If you are experiencing phone problems that you cannot resolve, Cisco TAC can assist you. You will need to turn debugging on for the phone, reproduce the problem, turn debugging off, and send the logs to TAC for analysis.

Because debugging captures detailed information, the communication traffic can slow down the phone, making it less responsive. After you capture the logs, you should turn debugging off to ensure phone operation.

The debug information may include a single digit code that reflects the severity of the situation. Situations are graded as follows:

- 0 - Emergency
- 1 - Alert
- 2 - Critical
- 3 - Error
- 4 - Warn
- 5 - Notification
- 6 - Information
- 7 - Debugging

Contact Cisco TAC for more information and assistance.

Procedure

Step 1 In the Cisco Unified Communications Manager Administration, select one of the following windows:

- **Device** > **Device settings** > **Common Phone Profile**

- **System** > **Enterprise Phone Configuration**
- **Device** > **Phone**

Step 2 Set the following parameters:

- Log Profile - values: Preset (default), Default, Telephony, SIP, UI, Network, Media, Upgrade, Accessory, Security, Energywise, MobileRemoteAccess
- Remote Log - values: Disable (default), Enable
- IPv6 Log Server or Log Server - IP address (IPv4 or IPv6 address)

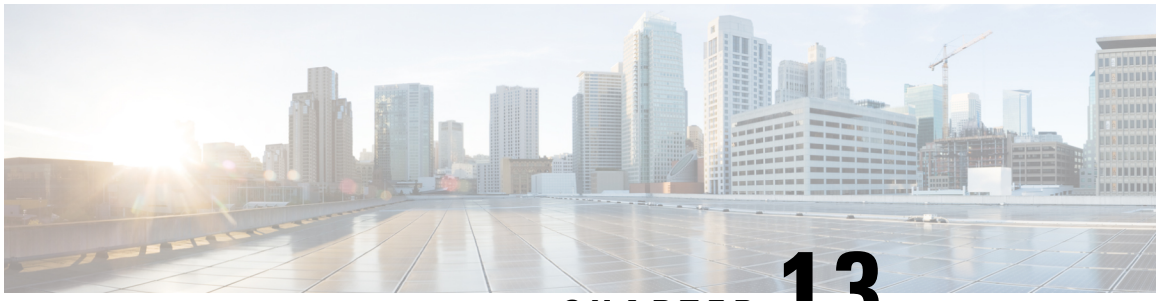
Note When the Log Server cannot be reached, the phone stops sending debug messages.

- The format for the IPv4 Log Server address is **`address:<port>@@base=<0-7>;pfs=<0-1>`**
- The format for the IPv6 Log Server address is **`[address]:<port>@@base=<0-7>;pfs=<0-1>`**
- Where:
  - the IPv4 address is separated with dot (.)
  - the IPv6 address is separated with colon (:)

Additional Troubleshooting Information

If you have additional questions about troubleshooting your phone, go to the following Cisco website and navigate to the desired phone model:

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



CHAPTER 13

Maintenance

Restart or Reset the Conference Phone

You perform a basic reset of a phone to recover if the phone experiences an error. You can also restore configuration and security settings to factory default settings.

Restart the Conference Phone

When you restart the phone, any user and network setup changes that aren't committed to the flash memory in the phone are lost.

Procedure

Press **Settings** > **Admin Settings** > **Reset settings** > **Reset device**.

Related Topics

Text and Menu Entry From the Phone, on page 41

Reset the Conference Phone Settings from the Phone Menu

Procedure

Step 1 Press **Settings**.

Step 2 Choose **Admin Settings** > **Reset Settings**.

Step 3 Select the type of reset.

- **All**—Restores the factory settings.
- **Reset device**—Resets the device. The existing settings don't change.

- **Network**—Resets the network configuration to default settings.
- **Service mode**—Clears the current service mode, deactivates the VPN and restarts the phone.
- **Security**—Resets the security configuration to default settings. This option deletes the CTL file.

Step 4 Press **Reset** or **Cancel**.

Related Topics

Text and Menu Entry From the Phone, on page 41

Reset the Conference Phone to Factory Defaults from the Keypad

When you reset the phone from the keypad, the phone reverts to the factory settings.

Procedure

Step 1 Unplug the phone:

- If using PoE, unplug the LAN cable.
- If using the power adapter, unplug the adapter.

Step 2 Wait 5 seconds.

Step 3 Press and hold **#**, and plug the phone back in.

Step 4 When the phone boots up, the LED strip lights up. As soon as the LED strip turns on, press **123456789*0#** in sequence.

After you press these buttons, the phone goes through the factory reset process.

If you press the buttons out of sequence, the phone powers on normally.

Caution Do not power down the phone until it completes the factory reset process, and the main screen appears.

Related Topics

Text and Menu Entry From the Phone, on page 41

Voice Quality Monitoring

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

- Concealment Ratio metrics—Show the ratio of concealment frames over total speech frames. An interval conceal ratio is calculated every 3 seconds.
- Concealed Second metrics—Show the number of seconds in which the DSP plays concealment frames due to lost frames. A severely “concealed second” is a second in which the DSP plays more than five percent concealment frames.

Note Concealment ratio and concealment seconds are primary measurements based on frame loss. A Conceal Ratio of zero indicates that the IP network is delivering frames and packets on time with no loss.

You can access voice quality metrics from the Cisco IP Phone using the Call Statistics screen or remotely by using Streaming Statistics.

Voice Quality Troubleshooting Tips

When you observe significant and persistent changes to metrics, use the following table for general troubleshooting information.

Table 31: Changes to Voice Quality Metrics

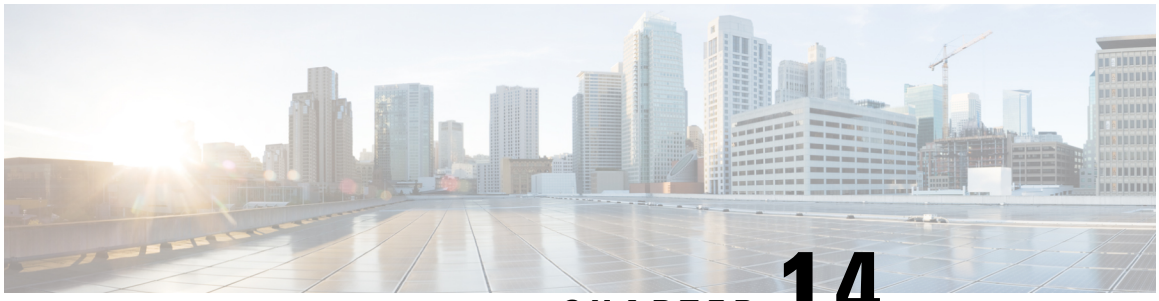
Metric Change	Condition
Conceal Ratio and Conceal Seconds increase significantly	Network impairment from packet loss or high jitter.
Conceal Ratio is near or at zero, but the voice quality is poor.	• Noise or distortion in the audio channel such as echo or audio levels. • Tandem calls that undergo multiple encode/decode such as calls to a cellular network or calling card network. • Acoustic problems coming from a speakerphone, handsfree cellular phone or wireless headset. Check packet transmit (TxCnt) and packet receive (RxCnt) counters to verify that voice packets are flowing.
MOS LQK scores decrease significantly	Network impairment from packet loss or high jitter levels: • Average MOS LQK decreases may indicate widespread and uniform impairment. • Individual MOS LQK decreases may indicate bursty impairment. Cross-check the conceal ratio and conceal seconds for evidence of packet loss and jitter.
MOS LQK scores increase significantly	• Check to see if the phone is using a different codec than expected (RxType and TxType). • Check to see if the MOS LQK version changed after a firmware upgrade.

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

Cisco IP Phone Cleaning

To clean your Cisco IP Phone, use only a dry soft cloth to gently wipe the phone and the phone screen. Do not apply liquids or powders directly to the phone. As with all non-weatherproof electronics, liquids and powders can damage the components and cause failures.

When the phone is in sleep mode, the screen is blank and the Select button is not lit. When the phone is in this condition, you can clean the screen, as long as you know that the phone will remain asleep until after you finish cleaning.



CHAPTER 14

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 the Software Download page, 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.

Related Topics

Cisco Unified Communications Manager Documentation, on page 14

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**.