REVIEW DRAFT - CISCO CONFIDENTIAL

Cisco Unified IP Phone 8961, 9951, and 9971 Administration Guide for Cisco Unified Communications Manager 10.0 (SIP)

First Published: August 16, 2013

Last Modified: August 22, 2013

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

CONTENTS

Preface

This document describes the administration of the Cisco Unified IP Phone 8961, 9951, and 9971.

Overview

Cisco Unified IP Phone 8961, 9951, and 9971 Administration Guide for Cisco Unified Communications Manager (SIP) provides the information you need to understand, install, configure, manage, and troubleshoot the phones on a VoIP network.

Because of the complexity of an IP telephony network, this guide does not provide complete and detailed information for procedures that you need to perform in Cisco Unified Communications Manager or other network devices.

Audience

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

Organization

The following table describes the organization of this manual.

Chapter	Description
Cisco Unified IP Phone, on page 1	Provides a conceptual overview and description of the Cisco Unified IP Phone.
Cisco Unified IP Phone and telephony networks, on page 41	Describes how the Cisco Unified IP Phone interacts with other key IP telephony components, and provides an overview of the tasks required before installation.
Cisco Unified IP Phone Installation, on page 55	Describes how to properly and safely install the Cisco Unified IP Phone on your network. Also provides procedures on how to configure and add accessories, such as Bluetooth wireless headsets, USB headsets, and analog wideband headsets, to the Cisco Unified IP Phone.
Cisco Unified IP Color Key Expansion Module Setup, on page 71	Describes how to connect and configure supported expansion modules for the Cisco Unified IP Phone.
Cisco Unified Video Camera setup, on page 79	Describes how to configure the Cisco Unified Video Camera and add it to the Cisco Unified IP Phone (Cisco Unified IP Phone 9951 and 9971 only).
VoIP Wireless Network, on page 83	Provides an overview and describes the setup of the wireless local area network (WLAN), which the Cisco Unified IP Phone 9971 supports.
Cisco Unified IP Phone Settings, on page 101	Describes how to configure network settings, verify status, and make global changes to the Cisco Unified IP Phone.
Features, Templates, Services, and User Setup, on page 129	Provides an overview of procedures for configuring telephony features, configuring directories, configuring phone button and softkey templates, setting up services, and adding users to Cisco Unified Communications Manager.
Cisco Unified IP Phone Customization, on page 211	Explains how to customize phone ring sounds and the phone idle display at your site.
Model information, status, and statistics, on page 225	Explains how to view model information, status messages, network statistics, and firmware information from the Cisco Unified IP Phone.
Remote Monitoring, on page 247	Describes the information that you can obtain from the web page for the phone to remotely monitor the operation of a phone and to assist with troubleshooting.
Troubleshooting and Maintenance, on page 267	Provides tips for troubleshooting the Cisco Unified IP Phone and the Cisco Unified IP Phone Expansion Modules.
Internal Support Website, on page 295	Provides suggestions for setting up a website for providing users with important information about their Cisco Unified IP Phones.

International User Support, on page 301	Provides information about setting up phones in non-English environments.
Technical Specifications, on page 303	Provides technical specifications of the Cisco Unified IP Phone.
Basic Phone Administration Steps, on page 307	Provides procedures for basic administration tasks such as adding a user and phone to Cisco Unified Communications Manager and then associating the user to the phone.
Cisco Unified IP Phone Wall Mount, on page 313	Contains instructions for installing the wall mount for the Cisco Unified IP Phone.
Cisco Unified IP Phone Non-Lockable Wall Mount, on page 325	Contains instructions for installing the Cisco Unified IP Phone Non-Lockable Wall Mount.

Related documentation

Use the following sections to obtain related information.

Cisco Unified IP Phone 8900 Series documentation

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

http://www.cisco.com/en/US/products/ps10451/tsd_products_support_series_home.html

Cisco Unified IP Phone 9900 Series documentation

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

http://www.cisco.com/en/US/products/ps10453/tsd_products_support_series_home.html

Cisco Unified Communications Manager documentation

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

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

Cisco Business Edition 3000 documentation

See the *Cisco Business Edition 3000 Documentation Guide* and other publications that are specific to your Cisco Business Edition 3000 release. Navigate from the following documentation URL:

http://www.cisco.com/en/US/products/ps11370/tsd_products_support_series_home.html

Cisco Business Edition 6000 documentation

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

http://www.cisco.com/en/US/products/ps11369/tsd_products_support_series_home.html

Documentation, support, and security guidelines

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

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

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

Cisco product security overview

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

Further information regarding U.S. export regulations may be found at http://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear.

Guide conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Convention	Description
`screen` font	Terminal sessions and information the system displays are in `screen` font.
input font	Information you must enter is in input font.
italic screen font	Arguments for which you supply values are in *italic screen* font.
^	The symbol ^ represents the key labeled Control - for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters such as passwords are in angle brackets.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

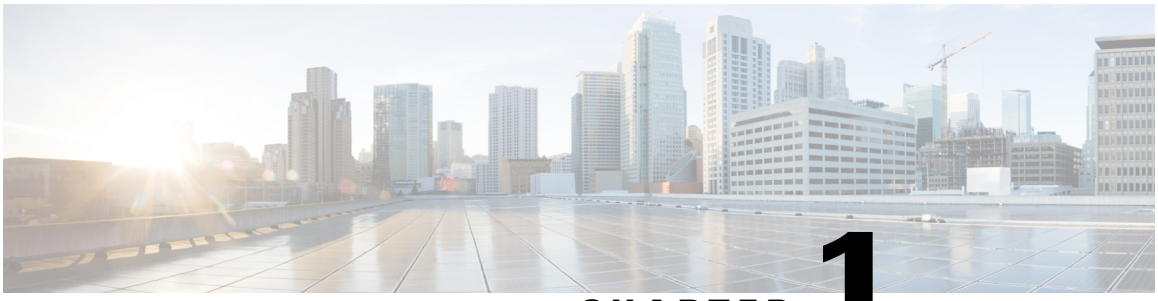
Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Warnings use the following convention:

Attention IMPORTANT SAFETY INSTRUCTIONS

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

SAVE THESE INSTRUCTIONS



CHAPTER 1

Cisco Unified IP Phone

The Cisco Unified IP Phone 8961, 9951, and 9971 provides voice communication over an Internet Protocol (IP) network. The Cisco Unified IP Phone functions much like a digital business phone, allowing you to place and receive phone calls and to access features such as mute, hold, transfer, speed dial, call forward, and more. In addition, because the phone connects to your data network, it offers enhanced IP telephony features, including access to network information and services, and customizeable features and services.

The Cisco Unified IP Phones have the following features:

- 24-bit color phone screen (Cisco Unified IP Phone 9971 has touchscreen support)
- Programmable feature buttons that support up to 5 lines (6 lines for the Cisco Unified IP Phone 9971) or that can be programmed for other features
- Full video capabilities (Cisco Unified IP Phones 9951 and 9971 only)
- Gigabit ethernet connectivity
- Support for an external microphone and speakers
- Bluetooth support for wireless headsets (Cisco Unified IP Phones 9951 and 9971 only)
- Network connectivity by Wi-Fi (Cisco Unified IP Phone 9971 only)
- USB ports:
  - two USB ports for Cisco Unified IP Phones 9951 and 9971
  - one USB port for Cisco Unified IP Phone 8961

A Cisco Unified IP Phone, like other network devices, must be configured and managed. These phones encode G.711 a-law, G.711 mu-law, G.722, G.729a, G.729ab, iLBC, and iSAC codecs, and decode G.711 a-law, G.711 mu-law, G.722, G.729, G.729a, G.729b, G.729ab, iLBC, and iSAC codecs.

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

This chapter includes the following topics:

Cisco Unified IP Phone 8961, 9951, and 9971

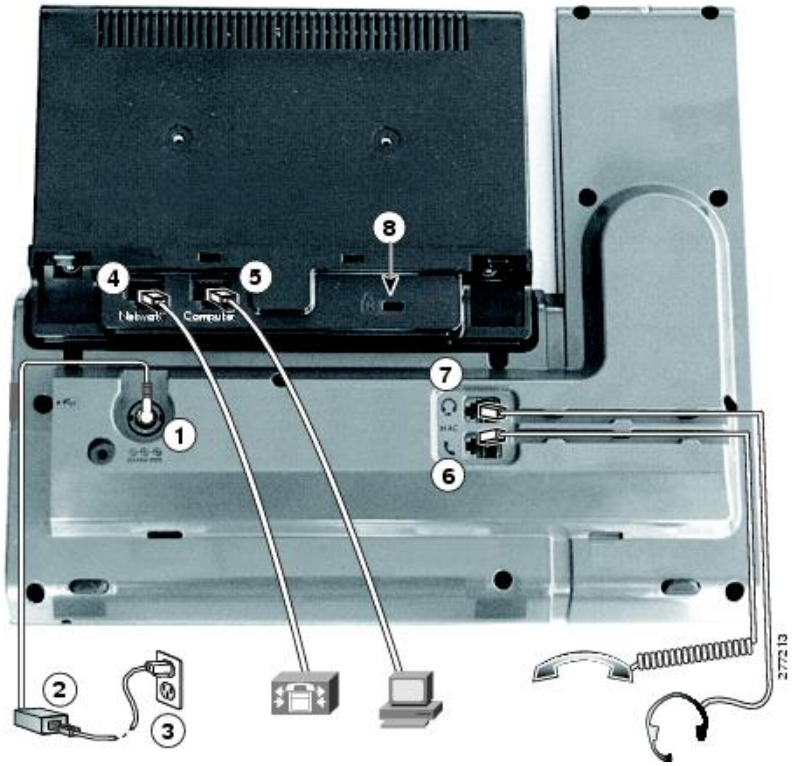
This section describes the Cisco Unified IP Phone 8961, 9951, and 9971 components. For more information, see *Cisco Unified IP Phone 8961, 9951, and 9971 User Guide for Cisco Unified Communications Manager*.

Cisco Unified IP Phone 8961

The following sections describe attributes of the Cisco Unified IP Phone 8961.

Phone Connections for Cisco Unified IP Phone 8961

Connect your phone to the corporate IP telephony network, using the following diagram.



1	DC adapter port (DC48V)	5	Computer port (10/100/1000 PC) connection

2	AC-to-DC power supply (optional)	6	Handset connection
3	AC power wall plug (optional)	7	Analog headset connection (headset optional)
4	Network port (10/100/1000 SW) with IEEE 802.3af and 802.3at power enabled	8	Anti-theft security lock connector (lock optional)

The following diagram shows the phone from the side.

1	USB port	2	Accessory connector; for example, to connect a Cisco Unified IP Color Key Expansion Module

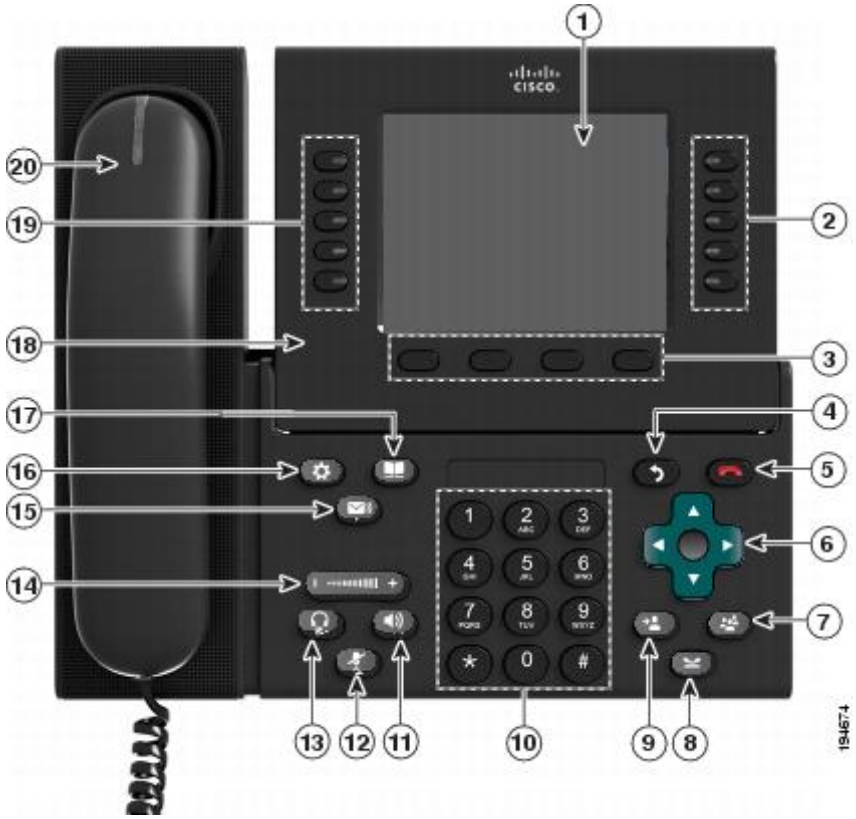
Note Each USB port supports the connection of up to five supported and nonsupported devices. Each device connected to the phone is included in the maximum device count. For example, the USB port on your phone can support a maximum of five USB devices (such as three Cisco Unified IP Color Key Expansion modules, one hub, and one other standard USB device). Many third-party USB products count as multiple USB devices, for example, a device containing USB hub and headset can count as two USB devices. For more information, see the USB device documentation.

Buttons and hardware

Your phone provides quick access to your phone lines, features, and call sessions:

- Programmable feature buttons (left side): Use to view calls on a line or access features such as Speed Dial or All Calls. (These buttons are also called feature buttons.)

- Session buttons (right side): Use to perform tasks such as answering a call, resuming a held call, or (when not being used for an active call) initiating phone functions such as displaying missed calls. Each call on your phone is associated with a session button.



1	Phone screen	Shows information about your phone, including directory number, call information (for example, caller ID, icons for an active call or call on hold) and available softkeys.

2	Session buttons 	Each button corresponds with an active call or a call function. When you press the button, the action depends on the state of the phone: • Active calls: Causes the phone to take the default action for an active call. For example, if you press the session button for a ringing call, the call is answered and if you press the button on a held call, the call resumes. Session information, such as caller ID and call duration, appears on the phone screen next to the session button. • Call functions: When a session button is not being used for an active call, it can be used to initiate functions on the phone, as indicated by the adjacent phone screen icons. For example, press the session button to display missed calls, take the phone off hook, or dial your voicemail system (with a Voicemail icon). Color LEDs reflect the call state. LEDs can *flash* (blink on and off rapidly), *pulse* (alternately dim and brighten), or appear solid (glow without interruption). • Flashing amber  : Ringing call. Press this button to answer the call. • Solid green  : May be a connected call or an outgoing call that is not yet connected. If the call is connected, press this button to display the call details or the participants of a conference call. If the call is not yet connected, press this button to end the call. • Pulsing green  : Held call. Press this button to resume the held call. • Solid red  : Shared line is in use remotely. Press this button to barge into call (if Barge is enabled). • Pulsing red  : Shared line call put on hold remotely. Press this button to resume the held call. The positions of the session buttons and feature buttons can be reversed on phones that use a locale with a right-to-left reading orientation, such as Hebrew and Arabic.
3	Softkey buttons 	Allow you to access the softkey options (for the selected call or menu item) displayed on your phone screen.
4	Back button 	Returns to the previous screen or menu.
5	Release button 	Ends a connected call or session.

6	Navigation pad and Select button 	The four-way Navigation pad allows you to scroll through menus, highlight items, and move within a text input field. The Select button (center of the Navigation pad) allows you to select a highlighted item. The Select button is lit (white) when the phone is in Power Save or Power Save Plus mode. Press the Select button to override Power Save and Power Save Plus mode.
7	Conference button 	Creates a conference call.
8	Hold button 	Places a connected call on hold and toggles between an active and held call.
9	Transfer button 	Transfers a call.
10	Keypad	Allows you to dial phone numbers, enter letters, and choose menu items by entering the item number.
11	Speakerphone button 	Selects the speakerphone as the default audio path and initiates a new call, picks up an incoming call, or ends a call. During a call, the button is lit green. The speakerphone audio path does not change until you select a new default audio path (for example, by picking up the handset). If external speakers are connected, the Speakerphone button selects them as the default audio path.
12	Mute button 	Toggles the microphone on or off during a call. When the microphone is muted, the button is lit red. When muted, you can hear the other parties on the call, but they cannot hear you.
13	Headset button 	Selects the headset as the default audio path and initiates a new call, picks up an incoming call, or ends a call. During a call, the button is lit green. A headset icon  in the phone screen header line indicates that the headset is the default audio path. This audio path does not change until you select a new default audio path (for example, by picking up the handset).

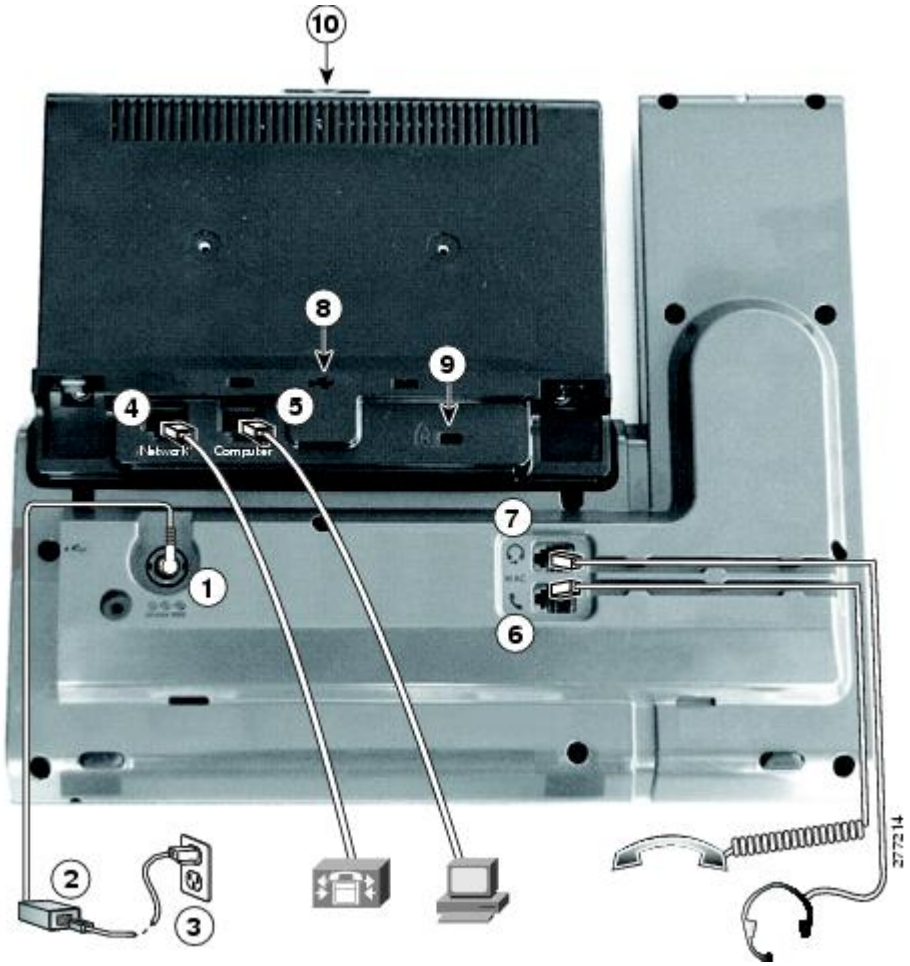
14	Volume button 	Controls the handset, headset, and speakerphone volume (off hook) and the ringer volume (on hook). Silences the ringer on the phone if an incoming call is ringing.
15	Messages button 	Autodials your voicemail system (varies by system).
16	Applications button 	Opens/closes the Applications menu. Depending on how your system administrator sets up the phone, use it to access applications such as call history, preferences, and phone information.
17	Contacts button 	Opens/closes the Contacts menu. Depending on how your system administrator sets up the phone, use it to access personal directory, corporate directory, or call history.
18	Phone display	Can be positioned to your preferred viewing angle.
19	Programmable feature buttons (also called feature buttons) 	Each button corresponds with a phone line, speed dial, or calling feature. Press a phone line button to display the active calls for that line. If you have multiple lines, you may have an All Calls button that displays a consolidated list of all calls from all lines (oldest at the top). If you do not see the All Calls button, your system administrator may have set up the primary line to automatically display all calls. For information on your set up, contact your system administrator. Color LEDs indicate the line state: • Amber  : Ringing call on this line • Green  : Active or held call on this line • Red  : Shared line in use remotely The positions of the session buttons and feature buttons can be reversed on phones that use a locale with a right-to-left reading orientation, such as Hebrew and Arabic.
20	Handset with light strip	The handset light strip lights up to indicate a ringing call (flashing red) or a new voice message (steady red).

Cisco Unified IP Phone 9951

The following sections describe attributes of the Cisco Unified IP Phone 9951.

Phone Connections for Cisco Unified IP Phone 9951

Connect your phone to the corporate IP telephony network, using the following diagram.



1	DC adapter port (DC48V)	6	Handset connection
2	AC-to-DC power supply (optional for the network port connection but required for a wifi connection)	7	Analog headset connection (headset optional)
3	AC power wall plug (optional)	8	USB port
4	Network port (10/100/1000 SW) with IEEE 802.3af and 802.3at power enabled	9	Anti-theft security connector (lock optional)
5	Computer port (10/100/1000 PC) connection	10	Camera pin holes (for Cisco Unified Video Camera)

The following picture shows the side of the phone.

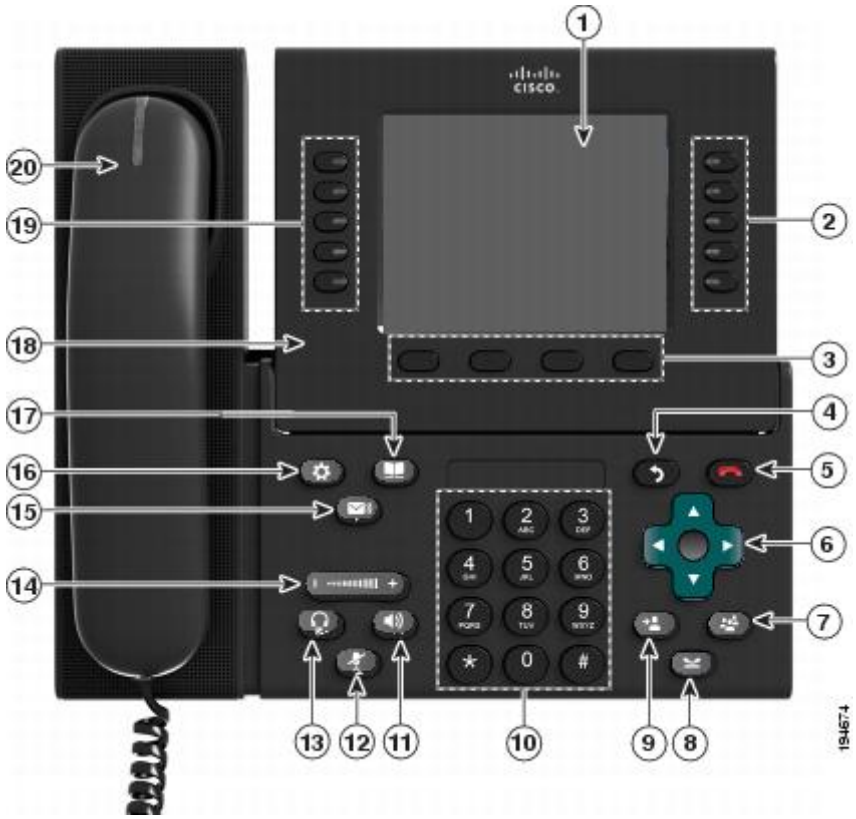
1	USB port	3	Speaker port for output to optional external speakers
2	Accessory connector; for example, for connecting a Cisco Unified IP Phone Expansion Module	4	Microphone port for input from optional external microphone

Note Each USB port supports a maximum of five supported and nonsupported devices that are connected to the phone. Each device connected to the phone is included in the maximum device count. For example, your phone can support five USB devices such as three Cisco Unified IP Color Key Expansion modules, one hub, and one other standard USB device on the side port and five additional standard USB devices on the back port. Many third-party USB products count as multiple USB devices, for example, a device containing USB hub and headset can count as two USB devices. For more information, see the USB device documentation.

Buttons and hardware

Your phone provides quick access to your phone lines, features, and call sessions:

- Programmable feature buttons (left side): Use to view calls on a line or access features such as Speed Dial or All Calls. These buttons are also called feature buttons.
- Session buttons (right side): Use to perform tasks such as answering a call, resuming a held call, or (when not being used for an active call) initiating phone functions such as displaying missed calls. Each call on your phone is associated with a session button.



1	Phone screen	Shows information about your phone, including directory number, call information (for example, caller ID, icons for an active call or call on hold) and available softkeys.

2	Session buttons 	Each button corresponds with an active call or a call function. When you press the button, the action depends on the state of the phone: • Active calls: Press the button to take the default action for an active call. For example, press the session button for a ringing call to answer the call and press the button on a held call to resume the call. Session information, such as caller ID and call duration, appears on the phone screen next to the session button. • Call functions: When a session button is not being used for an active call, it can be used to initiate functions on the phone, as indicated by the adjacent phone screen icons. For example, press the session button to display missed calls, take the phone off hook, or dial your voicemail system (with a Voicemail icon). Color LEDs reflect the call state. LEDs can *flash* (blink on and off rapidly), *pulse* (alternately dim and brighten), or appear solid (glow without interruption). • Flashing amber  : Ringing call. Press this button to answer the call. • Solid green  : May be a connected call or an outgoing call that is not yet connected. If the call is connected, press this button to display the call details or the participants of a conference call. If the call is not yet connected, press this button to end the call. • Pulsing green  : Held call. Press this button to resume the held call. • Solid red  : Shared line in use remotely. Press this button to barge into the call (if Barge is enabled). • Pulsing red  : Shared line call put on hold remotely. Press this button to resume the held call. The positions of the session buttons and feature buttons can be reversed on phones that use a locale with a right-to-left reading orientation, such as Hebrew and Arabic.
3	Softkey buttons 	Allow you to access the softkey options (for the selected call or menu item) displayed on your phone screen.
4	Back button 	Returns to the previous screen or menu.
5	Release button 	Ends a connected call or session.

6	Navigation pad and Select button 	The four-way Navigation pad allows you to scroll through menus, highlight items, and move within a text input field. The Select button (center of the Navigation pad) allows you to select a highlighted item. The Select button is lit (white) when the phone is in Power Save or Power Save Plus mode. Press the Select button to override Power Save and Power Save Plus mode.
7	Conference button 	Creates a conference call.
8	Hold button 	Places a connected call on hold and toggles between an ongoing and held call.
9	Transfer button 	Transfers a call.
10	Keypad	Allows you to dial phone numbers, enter letters, and choose menu items by entering the item number.
11	Speakerphone button 	Selects the speakerphone as the default audio path and initiates a new call, picks up an incoming call, or ends a call. During a call, the button is lit green. The speakerphone audio path does not change until you select a new default audio path (for example, by picking up the handset). If external speakers are connected, the Speakerphone button selects them as the default audio path.
12	Mute button 	Toggles the microphone on or off during a call. When the microphone is muted, the button is lit red. When muted, you can hear the other parties on the call, but they cannot hear you.
13	Headset button 	Selects the headset as the default audio path and initiates a new call, picks up an incoming call, or ends a call. During a call, the button is lit green. A headset icon  in the phone screen header line indicates the headset is the default audio path. This audio path does not change until you select a new default audio path (for example, by picking up the handset).

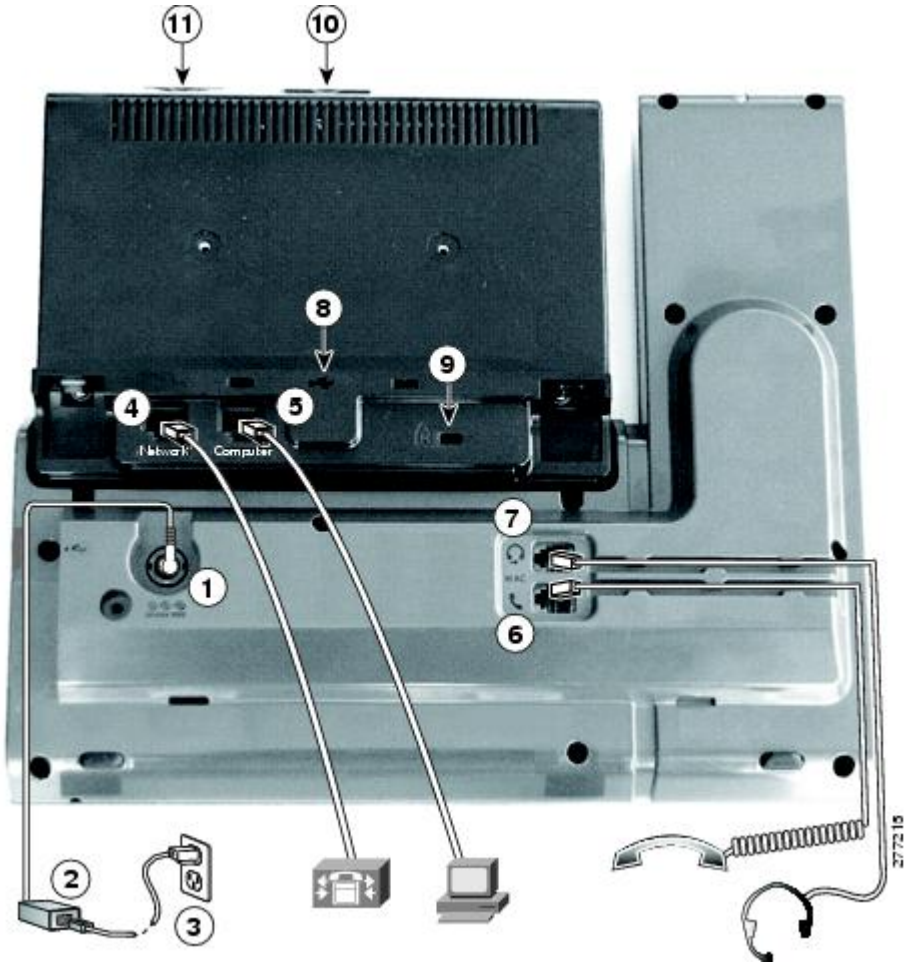
14	Volume button 	Controls the handset, headset, and speakerphone volume (off hook) and the ringer volume (on hook). Silences the ringer on the phone if an incoming call is ringing.
15	Messages button 	Autodials your voicemail system (varies by system).
16	Applications button 	Opens/closes the Applications menu. Depending on how your system administrator sets up the phone, use it to access applications such as call history, preferences, and phone information.
17	Contacts button 	Opens/closes the Contacts menu. Depending on how your system administrator sets up the phone, use it to access personal directory, corporate directory, or call history.
18	Phone display	Can be positioned to your preferred viewing angle.
19	Programmable feature buttons (also called feature buttons) 	Each button corresponds to a phone line, speed dial, and calling feature. Press a button for a phone line to display the active calls for that line. If you have multiple lines, you may have an All Calls button that displays a consolidated list of all calls from all lines (oldest at the top). If you do not see the All Calls button, your system administrator may have set up the primary line to automatically display all calls. For information on your set up, contact your system administrator. Color LEDs indicate the line state: • Amber  : Ringing call on this line • Green  : Active or held call on this line • Red  : Shared line in-use remotely The position of the programmable feature buttons can be reversed with the position of the session buttons on phones that use a locale with a right-to-left reading orientation, such as Hebrew and Arabic.
20	Handset with light strip	The handset light strip lights up to indicate a ringing call (flashing red) or a new voice message (steady red).

Cisco Unified IP Phone 9971

The following sections describe attributes of the Cisco Unified IP Phone 9971.

Phone Connections for Cisco Unified IP Phone 9971

Connect your phone to the corporate IP telephony network, using the following diagram.



1	DC adapter port (DC48V)	7	Analog headset connection (optional)
2	AC-to-DC power supply (optional for the network port connection but required for a Wi-Fi connection)	8	USB port
3	AC power wall plug (optional)	9	Anti-theft security lock connector (lock optional)
4	Network port (10/100/1000 SW) with IEEE 802.3af and 802.3at power enabled	10	Camera pin holes (for Cisco Unified Video Camera)

5	Computer port (10/100/1000 PC) connection	11	Secure Digital I/O (SDIO) slot (not used for this release)
6	Handset connection		

The following picture shows the side of the phone.

1	USB port	3	Speaker port for output to optional external speakers
2	Accessory connector; for example, for connecting a Cisco Unified IP Phone Expansion Module	4	Microphone port for input from optional external microphone

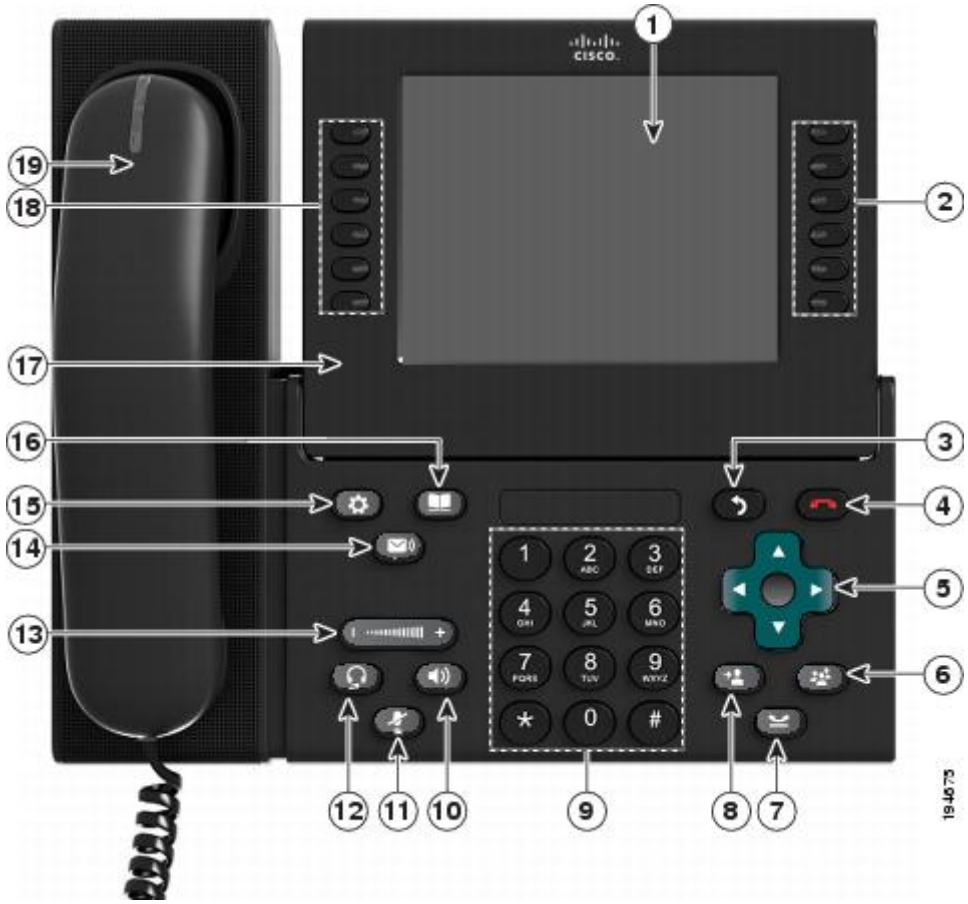
Note Each USB port supports the connection of up to five supported and nonsupported devices. Each device connected to the phone is included in the maximum device count. For example, your phone can support five USB devices (such as three Cisco Unified IP Color Key Expansion modules, one hub, and one other standard USB device) on the side port and five additional standard USB devices on the back port. Many third-party USB products count as multiple USB devices, for example, a device containing USB hub and headset can count as two USB devices. For more information, see the USB device documentation.

Buttons and hardware

Your phone provides quick access to your phone lines, features, and call sessions:

- Use the feature buttons (on the left) to view calls on a line or access features such as Speed Dial or All Calls.

- Use the call session buttons (on the right) to perform tasks such as making a call, answering a call, or resuming a held call. Each call on your phone is associated with a session button.



1	Phone screen	Shows information about your phone, including directory number, call information (for example, caller ID, icons for an active call or call on hold) and available softkeys. Phone screen items, such as menu options and softkeys, are touch-sensitive.

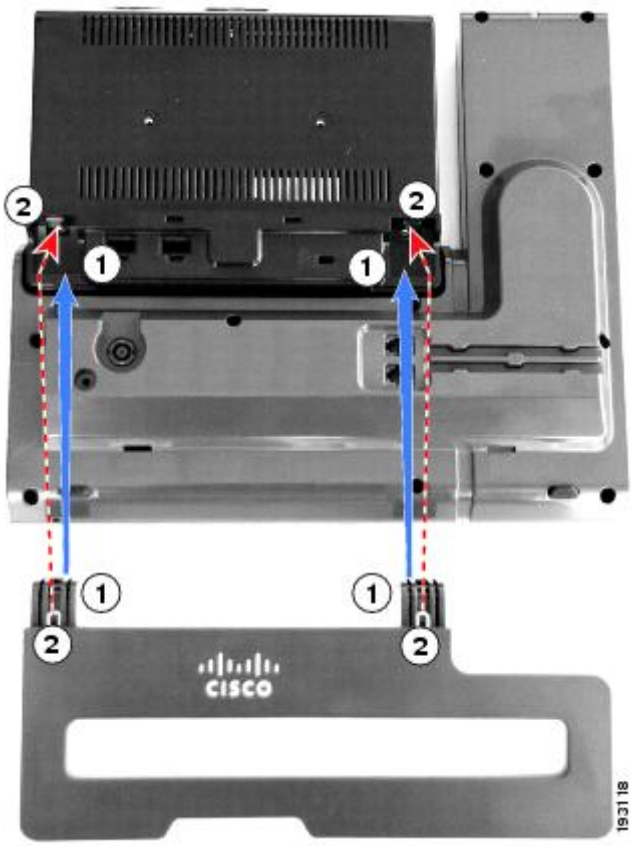
2	Session buttons 	Each button corresponds with an active call or a call function. When you press the button, the action depends on the state of the phone: • Active calls: Press the button to take the default action for an active call. For example, press the session button for a ringing call to answer the call and press the button on a held call to resume the call. Session information, such as caller ID and call duration, appears on the phone screen next to the session button. • Call functions: When a session button is not being used for an active call, it can be used to initiate functions on the phone, as indicated by the adjacent phone screen icons. For example, press the session button to display missed calls, take the phone off hook, or dial your voicemail system (with a Voicemail icon). Color LEDs reflect the call state. LEDs can *flash* (blink on and off rapidly), *pulse* (alternately dim and brighten), or appear solid (glow without interruption). • Flashing amber  : Ringing call. Press this button to answer the call. • Solid green  : May be a connected call or an outgoing call that is not yet connected. If the call is connected, press this button to display the call details or the participants of a conference call. If the call is not yet connected, press this button to end the call. • Pulsing green  : Held call. Press this button to resume the held call. • Solid red  : Shared line in use remotely. Press this button to barge into the call (if Barge is enabled). • Pulsing red  : Shared line call put on hold remotely. Press this button to resume the held call. The positions of the session buttons and feature buttons can be reversed on phones that use a locale with a right-to-left reading orientation, such as Hebrew and Arabic.
3	Back button 	Returns to the previous screen or menu.
4	Release button 	Ends a connected call or session.

5	Navigation pad and Select button 	The four-way Navigation pad allows you to scroll through menus, highlight items, and move within a text input field. The Select button (center of the Navigation pad) allows you to select a highlighted item, disable the phone screen for cleaning, or enable the phone screen if it is in power-save mode. The Select button is lit (white) when the phone is in Power Save or Power Save Plus mode. Press the Select button to override Power Save and Power Save Plus mode.
6	Conference button 	Creates a conference call.
7	Hold button 	Places a connected call on hold and toggles between an active and held call.
8	Transfer button 	Transfers a call.
9	Keypad	Allows you to dial phone numbers, enter letters, and choose menu items by entering the item number.
10	Speakerphone button 	Selects the speakerphone as the default audio path and initiates a new call, picks up an incoming call, or ends a call. During a call, the button is lit green. The speakerphone audio path does not change until you select a new default audio path (for example, by picking up the handset). If external speakers are connected, the Speakerphone button selects them as the default audio path.
11	Mute button 	Toggles the microphone on or off during a call. When the microphone is muted, the button is lit red. When muted, you can hear the other parties on the call, but they cannot hear you.
12	Headset button 	Selects the wired or wireless headset as the default audio path and initiates a new call, picks up an incoming call, or ends a call. During a call, the button is lit green. A headset icon  in the phone screen header line indicates the headset is the default audio path. This audio path does not change until a new default audio path is selected (for example, by picking up the handset).

13	Volume button 	Controls the handset, headset, and speakerphone volume (off hook) and the ringer volume (on hook). Silences the ringer on the phone if an incoming call is ringing.
14	Messages button 	Autodials your voicemail system (varies by system).
15	Applications button 	Opens/closes the Applications menu. Depending on how your system administrator sets up the phone, use it to access applications such as call history, preferences, and phone information.
16	Contacts button 	Opens/closes the Contacts menu. Depending on how your system administrator sets up the phone, use it to access personal directory, corporate directory, or call history.
17	Phone display	Can be positioned to your preferred viewing angle.
18	Programmable feature buttons (also called feature buttons) 	Correspond to phone lines, speed dials, and calling features. Press a button for a phone line to display the active calls for that line. If you have multiple lines, you may have an All Calls button that displays a consolidated list of all calls from all lines (oldest at the top). If you do not see the All Calls button, your system administrator may have set up the primary line to automatically display all calls. For information on your set up, contact your system administrator. Color LEDs indicate the line state: • Amber  : Ringing call on this line • Green  : Active or held call on this line • Red  : Shared line in-use remotely The positions of the session buttons and feature buttons can be reversed on phones that use a locale with a right-to-left reading orientation, such as Hebrew and Arabic.
19	Handset with light strip	The handset light strip lights up to indicate a ringing call (flashing red) or a new voice message (steady red).

Connect Footstand

If your phone is placed on a table or desk, connect the footstand to the back of the phone.



Procedure

Step 1 Insert the curved connectors into the lower slots.

Step 2 Lift the footstand until the connectors snap into the upper slots.

Note Connecting and disconnecting the footstand may require a little more force than you expect.

Phone and Cable Lock

You can secure the Cisco Unified IP Phone 8961, 9951, and 9971 to a desktop by using a laptop cable lock. The lock connects to the antitheft security connector on the back of the phone and the cable can be secured to a desktop.

The security slot can accommodate a lock up to 20 mm wide. Compatible laptop cable locks include the Kensington laptop cable lock and laptop cable locks from other manufacturers that can fit into the security slot on the back of the phone.

Network protocols

Cisco Unified IP Phones support several industry-standard and Cisco network protocols required for voice communication. The following table provides an overview of the network protocols that the Cisco Unified IP Phone 8961, 9951, and 9971 support.

Table 1: Supported network protocols on the Cisco Unified IP Phone

Network protocol	Purpose	Usage notes
Bluetooth	Bluetooth is a wireless personal area network (WPAN) protocol that specifies how devices communicate over short distances.	Cisco Unified IP Phones 9951 and 9971 support Bluetooth 2.1.
Bootstrap Protocol (BootP)	BootP enables a network device, such as the Cisco Unified IP Phone, to discover certain startup information, such as the IP address.	—
Cisco Audio Session Tunnel (CAST)	The CAST protocol allows Cisco Unified IP Phones and associated applications to discover and communicate with the remote IP Phones without requiring changes to the traditional signaling components, such as Cisco Unified Communications Manager (CM) and gateways.	The Cisco Unified IP Phone uses CAST as an interface between CUVA and Cisco Unified Communications Manager using the Cisco Unified IP Phone as a SIP proxy.
Cisco Discovery Protocol (CDP)	CDP is a device-discovery protocol that runs on all Cisco-manufactured equipment. Using CDP, a device can advertise its existence to other devices and receive information about other devices in the network.	The Cisco Unified IP Phone uses CDP to communicate information such as auxiliary VLAN ID, per port power management details, and Quality of Service (QoS) configuration information with the Cisco Catalyst switch.
Cisco Peer-to-Peer Distribution Protocol (CPPDP)	CPPDP is a Cisco proprietary protocol used to form a peer-to-peer hierarchy of devices. This hierarchy is used to distribute firmware files from peer devices to their neighboring devices.	CPPDP is used by the Peer Firmware Sharing feature.

Network protocol	Purpose	Usage notes
Dynamic Host Configuration Protocol (DHCP)	DHCP dynamically allocates and assigns an IP address to network devices. DHCP enables you to connect an IP phone into the network and the phone to become operational without the need to manually assign an IP address or to configure additional network parameters.	DHCP is enabled by default. If disabled, you must manually configure the IP address, subnet mask, gateway, and a TFTP server on each phone locally. Cisco recommends that you use DHCP custom option 150. With this method, you configure the TFTP server IP address as the option value. For additional supported DHCP configurations, see the "Dynamic Host Configuration Protocol" chapter and the "Cisco TFTP" chapter in the *Cisco Unified Communications Manager System Guide*. **Note** If you cannot use option 150, you may try using DHCP option 66.
Hypertext Transfer Protocol (HTTP)	HTTP is the standard way of transferring information and moving documents across the Internet and the web.	Cisco Unified IP Phones use HTTP for XML services and for troubleshooting purposes.
Hypertext Transfer Protocol Secure (HTTPS)	Hypertext Transfer Protocol Secure (HTTPS) is a combination of the Hypertext Transfer Protocol with the SSL/TLS protocol to provide encryption and secure identification of servers.	Web applications with both HTTP and HTTPS support have two URLs configured. Cisco Unified IP Phones that support HTTPS choose the HTTPS URL.
IEEE 802.1X	The IEEE 802.1X standard defines a client-server-based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. Until the client is authenticated, 802.1X access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.	The Cisco Unified IP Phone implements the IEEE 802.1X standard by providing support for the following authentication methods: EAP-FAST, EAP-TLS, and EAP-MD5. When 802.1X authentication is enabled on the phone, you should disable the PC port and voice VLAN. See 802.1X Authentication, on page 33 for additional information.
IEEE 802.11a/b/g	The IEEE 802.11 standard specifies how devices communication over a wireless local area network (WLAN). 802.11a operates at the 5 GHz band and 802.11b and 802.11g operate at the 2.4 GHz band	(Cisco Unified IP Phone 9971 only) The 802.11 interface is a deployment option for cases when Ethernet cabling is unavailable or undesirable.

Network protocol	Purpose	Usage notes
Internet Protocol (IP)	IP is a messaging protocol that addresses and sends packets across the network.	To communicate using IP, network devices must have an assigned IP address, subnet, and gateway. IP addresses, subnets, and gateway identifications are automatically assigned if you are using the Cisco Unified IP Phone with Dynamic Host Configuration Protocol (DHCP). If you are not using DHCP, you must manually assign these properties to each phone locally. The Cisco Unified IP Phones support IPv6 addresses. For more information, see *Cisco Unified Communications Manager Features and Services Guide*, "Internet Protocol Version 6 (IPv6)" chapter.
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 Cisco Unified IP 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 for voice products.	The Cisco Unified IP Phone supports LLDP-MED on the SW port to communicate information such as: • Voice VLAN configuration • Device discovery • Power management • Inventory management For more information about LLDP-MED support, see the LLDP-MED and Cisco Discovery Protocol white paper: http://www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper0900aecd804cd46d.shtml
Real-Time Transport Protocol (RTP)	RTP is a standard protocol for transporting real-time data, such as interactive voice and video, over data networks.	Cisco Unified IP Phones use the RTP protocol to send and receive real-time voice traffic from other phones and gateways.

Network protocol	Purpose	Usage notes
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 for audio calls is disabled by default. RTCP for video calls (including both audio streams and video streams in the video call) is enabled by default. You can enable or disable RTCP on individual phones from the Cisco Unified Communications Manager Administration.
Session Description Protocol (SDP)	SDP is the portion of the SIP protocol that determines which parameters are available during a connection between two endpoints. Conferences are established by using only the SDP capabilities that all endpoints in the conference support.	SDP capabilities, such as codec types, DTMF detection, and comfort noise, are normally configured on a global basis by Cisco Unified Communications Manager or Media Gateway in operation. Some SIP endpoints may allow configuration of these parameters on the endpoint itself.
Session Initiation Protocol (SIP)	SIP is the Internet Engineering Task Force (IETF) standard for multimedia conferencing over IP. SIP is an ASCII-based application-layer control protocol (defined in RFC 3261) that can be used to establish, maintain, and terminate calls between two or more endpoints.	Like other VoIP protocols, SIP addresses the functions of signaling and session management within a packet telephony network. Signaling allows transportation of call information across network boundaries. Session management provides the ability to control the attributes of an end-to-end call. Cisco Unified IP Phones support the SIP protocol when the phones are operating in IPv6 address, IPv4 address, or dual-stack mode.
Transmission Control Protocol (TCP)	TCP is a connection-oriented transport protocol.	Cisco Unified IP Phones use TCP to connect to Cisco Unified Communications Manager and to access XML services.
Transport Layer Security (TLS)	TLS is a standard protocol for securing and authenticating communications.	Upon security implementation, Cisco Unified IP Phones use the TLS protocol when securely registering with Cisco Unified Communications Manager.

Network protocol	Purpose	Usage notes
Trivial File Transfer Protocol (TFTP)	TFTP allows you to transfer files over the network. On the Cisco Unified IP Phone, TFTP enables you to obtain a configuration file specific to the phone type.	TFTP requires a TFTP server in your network that the DHCP server can automatically identify. If you want a phone to use a TFTP server other than the one that the DHCP server specifies, you must manually assign the IP address of the TFTP server by using the Network Configuration menu on the phone. For more information, see the "Cisco TFTP" chapter in the *Cisco Unified Communications Manager System Guide*.
User Datagram Protocol (UDP)	UDP is a connectionless messaging protocol for delivery of data packets.	UDP is used only for RTP streams. SIP signaling on the phones do not support UDP.

Related Topics

Set up audio and video port range, on page 201
Cisco Unified IP Communications Product Interactions, on page 41
Phone Startup Process, on page 48
Ethernet Setup menu, on page 104

Cisco Unified IP Phone Features

Cisco Unified IP Phones function much like a digital business phone, allowing you to place and receive phone calls. In addition to traditional telephony features, the Cisco Unified IP Phone includes features that enable you to administer and monitor the phone as a network device.

Feature Overview

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

As with other network devices, you must configure Cisco Unified 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 Unified 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 Unified 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.

Telephony Feature Administration

You can modify additional settings for the Cisco Unified IP Phone from Cisco Unified Communications Manager Administration. Use this web-based application to set up phone registration criteria and calling search spaces, to configure corporate directories and services, and to modify phone button templates, among other tasks. See the related topics and the Cisco Unified Communications Manager documentation for additional information.

For more information about Cisco Unified Communications Manager Administration, see Cisco Unified Communications Manager documentation, including *Cisco Unified Communications Manager Administration Guide*. You can also use the context-sensitive help available within the application for guidance.

You can access Cisco Unified Communications Manager documentation at this location:

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

You can access Cisco Unified Communications Manager Business Edition documentation at this location:

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

Related Topics

Telephony features available for Cisco Unified IP Phone, on page 130

Cisco Unified IP Phone Network Parameters

You can configure parameters such as DHCP, TFTP, and IP settings on the phone itself. You can also obtain statistics about a current call or firmware versions on the phone.

Information for End Users

If you are a system administrator, you are likely the primary source of information for Cisco Unified IP Phone users in your network or company. To ensure that you distribute the most current feature and procedural information, familiarize yourself with Cisco Unified IP Phone documentation. Make sure to visit the Cisco Unified IP Phone 8961, 9951, and 9971 web site:

http://www.cisco.com/en/US/products/ps10453/products_user_guide_list.html

From this site, you can view various user guides.

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

Cisco Unified IP Phone security features

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 Unified IP Phones.

The Cisco Unified IP Phone 8961, 9951, and 9971 uses 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 *Cisco Unified Communications Manager Security Guide*.

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 "Configuring Encrypted Phone Configuration Files" chapter in *Cisco Unified Communications Manager Security Guide*.

The following table shows where you can find information about security in this and other documents.

Table 2: Cisco Unified IP Phone and Cisco Unified Communications Manager security topics

Topic	Reference
Detailed explanation of security, including set up, configuration, and troubleshooting information for Cisco Unified Communications Manager and Cisco Unified IP Phones	See the *Cisco Unified Communications Manager Security Guide*.
Security features supported on the Cisco Unified IP Phone	See Supported security features, on page 28.
Restrictions regarding security features	See Security Restrictions, on page 34.
Viewing a security profile name	Supported security features, on page 28 provides an overview of the security features that the Cisco Unified IP Phone 8961, 9951, and 9971 supports. For more information about these features, about Cisco Unified Communications Manager, and about Cisco Unified IP Phone security, see the *Cisco Unified Communications Manager Security Guide*.
Identifying phone calls for which security is implemented	See Secure Phone Calls, on page 31.
Extension Mobility HTTPS Support	See Network protocols, on page 21.
TLS connection	See Network protocols, on page 21 and Cisco Unified Communications Manager Phone Addition Methods, on page 50.
Security and the phone startup process	See Phone Startup Process, on page 48.

Topic	Reference
Security and phone configuration files	See Cisco Unified Communications Manager Phone Addition Methods, on page 50.
Changing the TFTP Server 1 or TFTP Server 2 option on the phone when security is implemented.	See IPv4 Setup Menu Options, on page 113.
Items on the Security Setup menu that you access from the phone	See Security Setup Menu, on page 123.
Disabling access to the web pages for a phone	See Control web page access, on page 249.
Troubleshooting	See Cisco Unified IP Phone Security Problems, on page 273 and *Troubleshooting Guide for Cisco Unified Communications Manager*.
Deleting the CTL file from the phone	See Basic Reset, on page 290.
Resetting or restoring the phone	See Basic Reset, on page 290.
802.1X authentication for Cisco Unified IP Phones	See these sections: • 802.1X Authentication, on page 33 • Security Setup Menu, on page 123 • Status Menu, on page 227 • Cisco Unified IP Phone Security Problems, on page 273

Supported security features

The following table provides an overview of the security features that the Cisco Unified IP Phone 8961, 9951, and 9971 supports. For more information about these features, Cisco Unified Communications Manager, and Cisco Unified IP Phone security, see *Cisco Unified Communications Manager Security Guide*.

For information about current security settings on a phone, press  and choose **Administrator Settings** > **Security Setup**.

Table 3: Overview of Security Features

Feature	Description
Image authentication	Signed binary files (with the extension .sbn) prevent tampering with the firmware image before the image is loaded on a phone. Tampering with the image causes a phone to fail the authentication process and reject the new image.

Feature	Description
Image encryption	Encrypted binary files (with the extension .sebn) prevent tampering with the firmware image before the image is loaded on a phone. Tampering with the image causes a phone to fail the authentication process and reject the new image.
Customer site certificate installation	Each Cisco Unified IP Phone requires a unique certificate for device authentication. Phones include a manufacturing installed certificate (MIC), but for additional security, you can specify certificate installation in Cisco Unified Communications Manager Administration using the Certificate Authority Proxy Function (CAPF). Alternatively, you can install a Locally Significant Certificate (LSC) from the Security Configuration menu on the phone. See Cisco Unified IP Phone Security, on page 68 for more information.
Device authentication	Occurs between the Cisco Unified Communications Manager server and the phone when each entity accepts the certificate of the other entity. Determines whether a secure connection between the phone and a Cisco Unified Communications Manager should occur; and, if necessary, creates a secure signaling path between the entities by using TLS protocol. Cisco Unified Communications Manager does not register phones unless it can authenticate them.
File authentication	Validates digitally signed files that the phone downloads. The phone validates the signature to make sure that file tampering did not occur after file creation. Files that fail authentication are not written to Flash memory on the phone. The phone rejects such files without further processing.
File encryption	Encryption prevents sensitive information from being revealed while the file is in transit to the phone. In addition, the phone validates the signature to make sure that file tampering did not occur after file creation. Files that fail authentication are not written to Flash memory on the phone. The phone rejects such files without further processing.
Signaling authentication	Uses the TLS protocol to validate that no tampering to signaling packets has occurred during transmission.
Manufacturing installed certificate	Each Cisco Unified IP Phone contains a unique manufacturing installed certificate (MIC), which is used for device authentication. The MIC provides permanent unique proof of identity for the phone and allows Cisco Unified Communications Manager to authenticate the phone.
Media encryption	Uses SRTP to ensure that media streams between supported devices prove secure and that only the intended device receives and reads the data. Includes creating a media master key pair for the devices, delivering the keys to the devices, and securing the delivery of the keys while the keys are in transport.
CAPF (Certificate Authority Proxy Function)	Implements parts of the certificate generation procedure that are too processing-intensive for the phone, and interacts with the phone for key generation and certificate installation. The CAPF can be configured to request certificates from customer-specified certificate authorities on behalf of the phone, or it can be configured to generate certificates locally.

Feature	Description
Security profile	Defines whether the phone is nonsecure, authenticated, encrypted, or protected. Other entries in this table describe security features. For more information about these features, about Cisco Unified Communications Manager, and about Cisco Unified IP Phone security, see the *Cisco Unified Communications Manager Security Guide*.
Encrypted configuration files	Lets you ensure the privacy of phone configuration files.
Optional web server disabling for a phone	For security purposes, you can prevent access to the web pages for a phone (which display a variety of operational statistics for the phone) and User Options web pages. For more information, see Control web page access, on page 249.
Phone hardening	Additional security options, which you control from Cisco Unified Communications Manager Administration: • Disabling PC port • Disabling Gratuitous ARP (GARP) • Disabling PC Voice VLAN access • Disabling access to the Setting menus, or providing restricted access that allows access to the Preferences menu and saving volume changes only • Disabling access to web pages for a phone • Disabling Bluetooth Accessory Port
802.1X Authentication	The Cisco Unified IP Phone can use 802.1X authentication to request and gain access to the network. See 802.1X Authentication, on page 33 for more information.
Secure SIP Failover for SRST	After you configure a Survivable Remote Site Telephony (SRST) reference for security and then reset the dependent devices in Cisco Unified Communications Manager Administration, the TFTP server adds the SRST certificate to the phone cnf.xml file and sends the file to the phone. A secure phone then uses a TLS connection to interact with the SRST-enabled router.
Signaling encryption	Ensures that all SCCP and SIP signaling messages that are sent between the device and the Cisco Unified Communications Manager server are encrypted.

Security Profiles

All Cisco Unified IP Phones that support Cisco Unified Communications Manager use a security profile, which defines whether the phone is nonsecure, authenticated, or encrypted. For information about configuring the security profile and applying the profile to the phone, see *Cisco Unified Communications Manager Security Guide*.

To view the security mode that is set for the phone, look at the Security Mode setting in the Security Configuration menu.

Secure Phone Calls

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 and video (if video is involved). If your call connects to a nonsecure phone, the security tone does not play.

Note Secure calling is supported for connections between two phones only. Some features, such as conference calling, shared lines, and Extension Mobility, are not available when secure calling is configured.

The following sections describe call security.

Related Topics

Cisco Unified IP Phone security features, on page 27
Security Restrictions, on page 34

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 Interactions, restrictions, and limitations that affect the security level of the conference call depend on the security mode of the participant phones and the availability of secure conference bridges. See Call Security Interactions and Restrictions, on page 32 for information about these interactions.

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 and other multiple-line calls are not supported.

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. A security tone plays 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 nonsecured phone, the secure tone does not play.

Note Secured calling is supported for conversations between two phones. Some features, such as conference calling, shared lines, and Cisco Extension Mobility are not available when secured calling is configured.

Call Security Interactions and Restrictions

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. The following table provides information about changes to call security levels when using Barge.

Table 4: Call Security Interactions when using Barge

Initiator phone security level	Feature used	Call security level	Results of action
Nonsecure	Barge	Encrypted call	Call barged and identified as nonsecure call
Secure	Barge	Encrypted call	Call barged and identified as secure call

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 5: 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

Initiator phone security level	Feature used	Security level of participants	Results of action
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.

When using secure video over VPN and VXC/VPN, the maximum supported bandwidth is 320 kpbs.

When the phone calls Cisco TelePresence, the maximum bandwidth is 320 kbps.

802.1X Authentication

The Cisco Unified IP Phones support 802.1X Authentication.

Overview

Cisco Unified 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. CDP does not identify locally attached workstations. Cisco Unified IP Phones provide an EAPOL pass-through mechanism. This mechanism allows a workstation attached to the Cisco Unified IP Phone to pass EAPOL messages to the 802.1X authenticator at the LAN switch. The pass-through mechanism ensures that the IP phone does not act as the LAN switch to authenticate a data endpoint before accessing the network.

Cisco Unified IP Phones also provide a proxy EAPOL Logoff mechanism. In the event that the locally attached PC disconnects from the IP phone, the LAN switch does not see the physical link fail, because the link between the LAN switch and the IP phone is maintained. To avoid compromising network integrity, the IP phone sends an EAPOL-Logoff message to the switch on behalf of the downstream PC, which triggers the LAN switch to clear the authentication entry for the downstream PC.

Cisco Unified IP Phones also 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, EAP-TLS, and EAP-MD5 options for network authentication.

Required Network Components

Support for 802.1X authentication on Cisco Unified IP Phones requires several components, including:

- Cisco Unified IP Phone: The phone acts as the 802.1X *supplicant*, which initiates the request to access the network.

- Cisco Secure Access Control Server (ACS) (or other third-party authentication server): The authentication server and the phone must both be configured with a shared secret that authenticates the phone.
- 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.

Best Practices

The following list describes requirements and recommendations for 802.1X configuration.

- Enable 802.1X Authentication: If you want to use the 802.1X standard to authenticate Cisco Unified IP Phones, be sure that you properly configure the other components before enabling it on the phone.
- Configure PC Port: The 802.1X standard does not take into account the use of VLANs and thus recommends that only a single device should be authenticated to a specific switch port. However, some switches (including Cisco Catalyst switches) support multidomain authentication. The switch configuration determines whether you can connect a PC to the PC port of the phone.
  - Enabled: If you are using a switch that supports multidomain authentication, you can enable the PC port and connect a PC to it. In this case, Cisco Unified IP Phones support proxy EAPOL-Logoff to monitor the authentication exchanges between the switch and the attached PC. For more information about IEEE 802.1X support on the Cisco Catalyst switches, see the Cisco Catalyst switch configuration guides at:

    http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html
  - Disabled: If the switch does not support multiple 802.1X-compliant devices on the same port, you should disable the PC Port when 802.1X authentication is enabled. If you do not disable this port and subsequently attempt to attach a PC to it, the switch denies network access to both the phone and the PC.
- 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.
- Enter MD5 Shared Secret: If you disable 802.1X authentication or perform a factory reset on the phone, the previously configured MD5 shared secret is deleted.

Related Topics

Ethernet Setup menu, on page 104
802.1X Authentication and Transaction Status, on page 125

Security Restrictions

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.

Cisco Unified IP Phone Deployment

When deploying 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 "System Configuration Overview" chapter in *Cisco Unified Communications Manager System Guide*.

After you set up the IP telephony system and configure systemwide features in Cisco Unified Communications Manager, you can add IP phones to the system.

Cisco Unified IP Phone Setup in Cisco Unified Communications Manager

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

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

For general information about configuring phones in Cisco Unified Communications Manager, see the following documentation:

- "Cisco Unified IP Phones" chapter in the *Cisco Unified Communications Manager System Guide*
- "Cisco Unified IP Phone configurations" chapter in the *Cisco Unified Communications Manager Administration Guide*.
- "Autoregistration configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*.
- *Cisco Unified Communications Manager Bulk Administration Guide*.

Related Topics

Cisco Unified Communications Manager Phone Addition Methods, on page 50

Set up Cisco Unified IP Phone 8961, 9951, and 9971 in Cisco Unified Communications Manager

The following steps provide an outline of configuration tasks for the Cisco Unified IP Phone 8961, 9951, and 9971 in Cisco Unified Communications Manager Administration. The steps present a suggested order to guide you through the phone configuration process. Some tasks are optional, depending on your system and user needs. For detailed procedures and information, see the sources in the steps.

Procedure

Step 1 Gather the following information about the phone:

- Phone model
- MAC address
- Physical location of the phone
- Name or user ID of phone user
- Device pool
- Partition, calling search space, and location information
- Number of lines and associated directory numbers (DNs) to assign to the phone
- Cisco Unified Communications Manager user to associate with the phone
- Phone usage information that affects phone button template, phone features, IP Phone services, or phone applications

The information provides a list of configuration requirements for setting up phones and identifies preliminary configuration that you need to perform before configuring individual phones, such as phone button templates.

For more information, see the "Cisco Unified IP Phones" chapter in the *Cisco Unified Communications Manager System Guide* and Telephony features available for Cisco Unified IP Phone, on page 130.

Step 2 Verify that you have sufficient unit licenses for your phone. For more information, see the "Licensing" section in the *Cisco Unified Communications Manager System Guide*.

Step 3 Customize phone button templates (if required) by changing the number of line buttons, speed-dial buttons or service URL buttons. You can add a Privacy, All Calls, or Mobility button to meet user needs.
For more information, see the "Phone Button Template Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide* and Phone Button Templates, on page 173.

Step 4 Add and configure the phone by completing the required fields in the Phone Configuration window. An asterisk (*) next to the field name indicates a required field; for example, MAC address and device pool.
This step adds the device with the default settings to the Cisco Unified Communications Manager database.

For more information, see the "Cisco Unified IP Phone Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*.

For information about product-specific configuration fields, see the "?" Button Help in the Phone Configuration window.

Note If you want to add both the phone and user to the Cisco Unified Communications Manager database at the same time, see the "User/Phone Add Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*.

Step 5 Add and configure directory numbers (lines) on the phone by completing the required fields in the Directory Number Configuration window. An asterisk (*) next to the field name indicates a required field; for example, directory number and presence group.
This step adds primary and secondary directory numbers and features associated with directory numbers to the phone.

For more information, see the "Directory Number Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide* and Telephony features available for Cisco Unified IP Phone, on page 130.

Step 6 Configure speed-dial buttons and assign speed-dial numbers.
Users can change speed-dial settings on their phones by using Cisco Unified Communications Manager User Options.

For more information, see the "Configuring Speed-Dial Buttons or Abbreviated Dialing" section in the "Cisco Unified IP Phone Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*.

Step 7 Configure Cisco Unified IP Phone services and assign services (optional) to provide IP Phone services.
Users can add or change services on their phones by using the Cisco Unified Communications Manager User Options web pages.

Note Users can subscribe to the IP Phone service only if the Enterprise Subscription check box is unchecked when the IP Phone service is first configured in Cisco Unified Communications Manager Administration.

Note Some Cisco-provided default services are classified as enterprise subscriptions, so the user cannot add them through the User Options web pages. Such services are on the phone by default, and they can only be removed from the phone if you disable them in Cisco Unified Communications Manager Administration.

For more information, see the "IP Phone Services Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide* and Services Setup, on page 180.

Step 8 Assign services to programmable buttons (optional) to provide access to an IP Phone service or URL.
For more information, see the "Adding a Service URL Button" section of the "Cisco Unified IP Phone Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*.

Step 9 Add user information by configuring required fields. An asterisk (*) next to the field name indicates a required field; for example, User ID and last name. This step adds user information to the global directory for Cisco Unified Communications Manager.

Note Assign a password (for User Options web pages) and PIN (for Cisco Extension Mobility and Personal Directory).

For more information, see the "End User Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide* and Add Users to Cisco Unified Communications Manager, on page 181.

Note If your company uses a a Lightweight Directory Access Protocol (LDAP) directory to store information about users, you can install and configure Cisco Unified Communications to use your existing LDAP directory, see Corporate Directory setup, on page 168.

Note If you want to add both the phone and user to the Cisco Unified Communications Manager database at the same time, see the "User/Phone Add Configurations" chapter in the *Cisco Unified Communications Manager Administration Guide*.

Step 10 Associate a user to a user group. This step 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. For example, you must add users to the standard Cisco CCM End Users group so users can access Cisco Unified Communications Manager User Options.
For more information, see the following sections in the *Cisco Unified Communications Manager Administration Guide*:

- "End User Configuration Settings" section in the "End User Configuration" chapter
- "Adding Users to a User Group" section in the "User Group Configuration" chapter

Step 11 Associate a user with a phone (optional). This step provides users with control over their phone such a forwarding calls or adding speed-dial numbers or services.

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

For more information, see the "Associating Devices to an End User" section in the "End User Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*.

Cisco Unified IP Phone Installation

After you add phones to the Cisco Unified Communications Manager database, you can complete the phone installation. You (or the phone users) can install the phone at the user location. The *Cisco Unified IP Phone Installation Guide*, which is provided on the Cisco.com website, provides directions for connecting the phone handset, cables, and other accessories.

Note Before you install a phone, even if it is new, upgrade the phone to the current firmware image. For information about upgrading, see the Readme file for your phone, which is located at:

http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=278875240

After the phone connects to the network, the phone startup process begins, and the phone registers with Cisco Unified Communications Manager. To finish installing the phone, configure the network settings on the phone depending on whether you enable or disable DHCP service.

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

Set up Cisco Unified IP Phone 8961, 9951, and 9971

The following steps provide an overview and checklist of installation tasks for the Cisco Unified IP Phone 8961, 9951, and 9971. The list presents a suggested order to guide you through the phone installation. Some tasks are optional, depending on your system and user needs. For detailed procedures and information, see the sources in the steps.

Procedure

Step 1 Choose the power source for the phone:

- Power over Ethernet (PoE)
- External power supply

Note The Cisco Unified IP Phone 9971 requires an external power supply when used in a WLAN environment.

For more information, see Cisco Unified IP Phone Power, on page 43.

Step 2 Assemble the phone, adjust phone placement, and connect the network cable. If you are using the Cisco Unified IP Phone 9971 in a WLAN environment, see Step 5.
This step locates and installs the phone in the network. For more information, see Connect Footstand, on page 19 and Install Cisco Unified IP Phone, on page 66.

Step 3 Monitor the phone startup process. This step adds primary and secondary directory numbers and features that are associated with directory numbers to the phone, and verifies that the phone is configured properly.
For more information, see Phone Startup Verification, on page 68.

Step 4 If you choose to deploy the Cisco Unified IP Phone 9971 on a wireless network, skip to Step 5.
If you are configuring the Ethernet network settings on the phone for an IP network, you can set up an IP address for the phone either by using DHCP or by manually entering an IP address. For more information, see Network Settings, on page 68, Ethernet Setup menu, on page 104, and DHCP Usage, on page 118.

Step 5 (Cisco Unified IP Phone 9971 only) If you choose to deploy the Cisco Unified IP Phone 9971 on the wireless network, you must perform the following:

- Configure the wireless network.
- Enable wireless LAN for phones on Cisco Unified Communications Manager Administration.
- Configure a wireless network profile on the phone.

Note The wireless LAN on the phone does not activate when Ethernet cables are connected on the phone.

For more information, see VoIP Wireless Network, on page 83.

Step 6 Make calls with the Cisco Unified IP Phone to verify that the phone and features work correctly.
See the *Cisco Unified IP Phone 8961, 9951, and 9971 User Guide for Cisco Unified Communications Manager*.

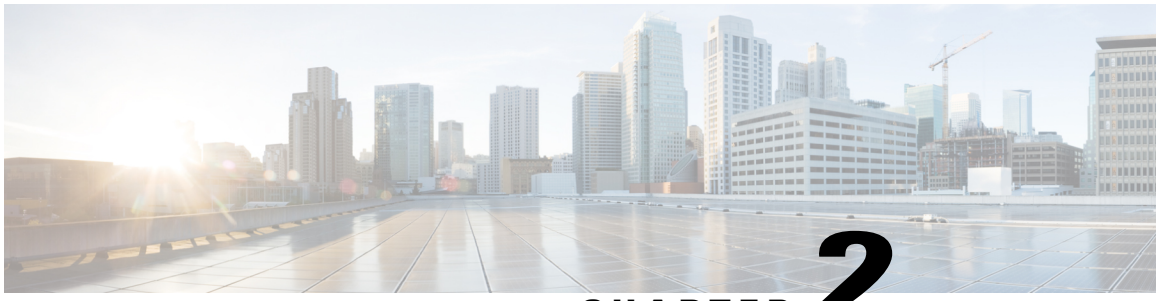
Step 7 Provide information to end users about how to use their phones and how to configure their phone options. This step ensures that users have adequate information to successfully use their Cisco Unified IP Phones.
For more information, see Internal Support Website, on page 295

Terminology differences

The following table highlights some of the differences in terminology found in the *Cisco Unified IP Phone 8961, 9951, and 9971 User Guide for Cisco Unified Communications Manager (SIP)*, the *Cisco Unified IP Phone 8961, 9951, and 9971 Administration Guide for Cisco Unified Communications Manager (SIP)*, and the *Cisco Unified Communications Manager Administration Guide*.

Table 6: Terminology differences

User Guide	Administration Guide
Line Status	Busy Lamp Field (BLF)
Message Indicators	Message Waiting Indicator (MWI) or Message Waiting Lamp
Programmable Feature Button	Programmable Button or Programmable Line Key (PLK)
Simplified New Call Window	Simplified New Call Bubble
Voicemail System	Voice Messaging System



CHAPTER 2

Cisco Unified IP Phone and telephony networks

Cisco Unified IP Phones enable you to communicate by using voice over a data network. To provide this capability, IP phones depend upon and interact with several other key Cisco Unified IP Telephony components, including Cisco Unified Communications Manager.

This chapter focuses on the interactions between the Cisco Unified IP Phone 8961, 9951, and 9971 and Cisco Unified Communications Manager, DNS and DHCP servers, TFTP servers, and switches. The chapter also describes phone power options.

For related information about voice and IP communications, see this URL:

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

This chapter provides an overview of the interaction between the Cisco Unified IP Phone and other key components of the VoIP network. The chapter includes the following topics:

Cisco Unified IP Communications Product Interactions

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

Cisco Unified IP Phone and Cisco Unified Communications Manager Interaction

Cisco Unified Communications Manager is an open, industry-standard call processing system. Cisco Unified Communications Manager software sets up and tears down calls between phones, integrating traditional PBX functionality with the corporate IP network. Cisco Unified Communications Manager manages

the components of the IP telephony system, such as the phones, the access gateways, and the resources necessary for features such as call conferencing and route planning. Cisco Unified Communications Manager also provides:

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

For information about configuring Cisco Unified Communications Manager to work with the IP devices described in this chapter, see the "Cisco Unified IP Phone Configuration" chapter in the *Cisco Communications Manager Administration Guide*.

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

http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml

Cisco Unified IP Phone and VLAN Interaction

The Cisco Unified IP Phone 8961, 9951, and 9971 contains an internal Ethernet switch, enabling forwarding of packets to the phone, and to the computer (access) port and the network port on the back of the phone.

If a computer is connected to the computer (access) port, the computer and the phone share the same physical link to the switch and share the same port on the switch. This shared physical link has the following implications for the VLAN configuration on the network:

- The current VLANs might be configured on an IP subnet basis. However, additional IP addresses might not be available to assign the phone to the same subnet as other devices that connect to the same port.
- Data traffic present on the VLAN supporting phones might reduce the quality of VoIP traffic.
- Network security may indicate a need to isolate the VLAN voice traffic from the VLAN data traffic.

You can resolve these issues by isolating the voice traffic onto a separate VLAN. The switch port to which the phone connects would be configured for separate VLANs for carrying:

- Voice traffic to and from the IP phone (auxiliary VLAN on the Cisco Catalyst 6000 series, for example)
- Data traffic to and from the PC that connects to the switch through the computer (access) port of the IP phone (native VLAN)

Isolating the phones on a separate, auxiliary VLAN increases the quality of the voice traffic and allows a large number of phones to be added to an existing network that does not have enough IP addresses for each phone.

For more information, see the documentation that is included with a Cisco switch. You can also access switch information at this URL:

http://cisco.com/en/US/products/hw/switches/index.html

Cisco Unified IP Phone and Cisco Unified Communications Manager Express Interaction

When the Cisco Unified IP Phone works with the Cisco Unified Communications Manager Express (Unified CME), the phones 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 Cisco Unified IP 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

Not supported.

Direct Transfer

Not supported.

Select

Not supported.

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

Cisco Unified IP Phone Power

The Cisco Unified IP Phone 8961, 9951, and 9971 can be powered with external power or with Power over Ethernet (PoE). A separate power supply provides external power. The switch can provide PoE through the phone Ethernet cable.

Note When you install a phone that is powered with external power, connect the power supply to the phone and to a power outlet before you connect the Ethernet cable to the phone. When you remove a phone that is powered with external power, disconnect the Ethernet cable from the phone before you disconnect the power supply.

Power Guidelines

The following table provides guidelines for Cisco Unified IP Phone 8961, 9951, and 9971 power.

Table 7: Guidelines for Cisco Unified IP Phone 8961, 9951, and 9971 Power

Power type	Guidelines
External power: Provided through the CP-PWR-CUBE-4= external power supply	The Cisco Unified IP Phone 8961, 9951, and 9971 uses the CP-PWR-CUBE-4 power supply. **Note** You must use the CP-PWR-CUBE-4 when you deploy the Cisco Unified IP Phone 9971 on a wireless network.
External power—Provided through the Cisco Unified IP Phone Power Injector.	The Cisco Unified IP Phone Power Injector may be used with any Cisco Unified IP Phone. Functioning as a midspan device, the injector delivers inline power to the attached phone. The Cisco Unified IP Phone Power Injector connects between a switch port and the IP Phone, and supports a maximum cable length of 100m between the unpowered switch and the IP phone.
PoE power—Provided by a switch through the Ethernet cable attached to the phone.	Cisco Unified IP Phone 8961, 9951, and 9971 supports IEEE 802.3af Class 3 power on signal pairs and spare pairs. Cisco Unified IP Phone 8961, 9951, and 9971 supports IEEE 802.3at for external add-on devices. To ensure uninterruptible operation of the phone, make sure that the switch has a backup power supply. Make sure 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. Support for NG-PoE+: The Cisco Unified IP Phone 8961, 9951, and 9971 can draw more power than IEEE 802.3at, as long as there is NG-PoE+ switch support.

Power Outage

Your access to emergency service through the phone requires the phone to receive power. If an interruption in the power supply occurs, Service and Emergency Calling Service dialing do not function until power is restored. In the case of a power failure or disruption, you may need to reset or reconfigure equipment before you can use the Service or Emergency Calling Service dialing.

Phone Power Reduction

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

Power Save mode

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 lifts the handset or presses any button. In the Phone Configuration window on Cisco Unified Communications Manager Administration, configure the following parameters:

Days Display Not Active

Specifies the days that the backlight remains inactive.

Display on Time

Schedules the time of day that the backlight automatically activates. on the days listed in the off schedule.

Display on Duration

Indicates the length of time that the backlight is active after the backlight is enabled by the programmed schedule.

Display Idle Timeout

Defines the period of user inactivity on the phone before the backlight is turned off.

EnergyWise Mode

In addition to Power Save mode, the Cisco Unified 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. In the Phone Configuration window in Cisco Unified Communications Manager Administration, configure the following parameters:

Enable Power Save Plus

Selects the schedule of days for which the phone powers off.

Phone On Time

Determines when the phone automatically turns on for the days that are selected in the Enable Power Save Plus field.

Phone Off Time

Determines the time of day that the phone powers down for the days that are selected in the Enable Power Save Plus field.

Phone Off Idle Timeout

Determines the length of time that the phone must be idle before the phone powers down.

Enable Audio Alert

When enabled, instructs the phone to play an audible alert starting 10 minutes before the time that the Phone Off Time field specifies.

EnergyWise Domain

Specifies the EnergyWise domain that the phone is in.

EnergyWise Secret

Specifies the security secret password that is used to communicate within the EnergyWise domain.

Allow EnergyWise Overrides

Determines whether you allow the EnergyWise domain controller policy to send power-level updates to the phones.

When a phone is sleeping, the power sourcing equipment (PSE) provides minimal power to the phone to illuminate the Select key, and the Select key can be used to wake up the phone when it is sleeping.

Power Negotiation over LLDP

The phone and the switch negotiate the power that the phone consumes. Cisco Unified IP Phone 8961, 9951, and 9971 operates at multiple power settings, which lowers power consumption when less power is available.

After a phone reboots, the switch locks to one protocol (CDP or LLDP) for power negotiation. The switch locks to the first protocol (containing a power Threshold Limit Value [TLV]) that the phone transmits. If the system administrator disables that protocol on the phone, the phone cannot power up any accessories because the switch does not respond to power requests in the other protocol.

Cisco recommends that Power Negotiation always be enabled (default) when connecting to a switch that supports power negotiation.

If Power Negotiation is disabled, the switch may disconnect power to the phone. If the switch does not support power negotiation, disable the Power Negotiation feature before you power up accessories over PoE. When the Power Negotiation feature is disabled, the phone can power the accessories up to the maximum that the IEEE 802.3af-2003 standard allows.

Note When CDP and Power Negotiation are disabled, the phone can power the accessories up to 15.4W.

Additional Information About Power

The documents in the following table provide more information on the following topics:

- Cisco switches that work with Cisco Unified IP Phones
- Cisco IOS releases that support bidirectional power negotiation
- Other requirements and restrictions about power

Document topics	URL
Cisco Unified IP Phone Power Injector	http://www.cisco.com/en/US/products/ps6951/index.html
PoE Solutions	http://www.cisco.com/en/US/netsol/ns340/ns394/ns147/ns412/index.html
Cisco Catalyst Switches	http://www.cisco.com/en/US/products/hw/switches/index.html
Integrated Service Routers	http://www.cisco.com/en/US/products/hw/routers/index.html
Cisco IOS Software	http://www.cisco.com/en/US/products/sw/iosswrel/products_ios_cisco_ios_software_category_home.html

Phone Configuration Files

The TFTP server stores the phone configuration files that 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 configuration file for the phone.

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

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

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

Note If the device security mode in the configuration file is set to Authenticated or Encrypted, but the phone has not received a CTL or ITL file, the phone makes four attempts to obtain the file so the phone can register securely.

If autoregistration is not enabled and the phone does not exist in the Cisco Unified Communications Manager database, the system rejects the phone registration request and a blank screen displays.

If the phone has registered previously, the phone accesses the SEPmac_address.cnf.xml configuration file, where mac_address is the MAC address of the phone.

The filenames are derived from the MAC address and description fields in the Phone Configuration window of Cisco Unified Communications Manager Administration. The MAC address uniquely identifies the phone.

Phone Startup Process

When connecting to the VoIP network, the Cisco Unified IP Phone 8961, 9951, and 9971 goes through a standard startup process. Depending on your specific network configuration, only some of these steps may occur on your Cisco Unified IP Phone.

1. Obtain power from the switch. If a phone is not using external power, the switch provides inline power through the Ethernet cable that is attached to the phone.

   For more information, see Cisco Unified Communications Manager Phone Addition Methods, on page 50 and Startup Problems, on page 267.

2. (For a Cisco Unified IP Phone 9971 in a wireless LAN only) Scan for an access point. The Cisco Unified IP Phone 9971 scans the RF coverage area with the radio. The phone searches the network profiles and scans for access points that contain a matching SSID and authentication type. The phone associates with the access point with the highest RSSI that matches with the network profile.

   For more information, see Cisco Unified Wireless AP Interactions, on page 90.

3. (For a Cisco Unified IP Phone 9971 in a wireless LAN only) Authenticate with the access point. The Cisco Unified IP Phone begins the authentication process. The following table describes the authentication process:

Authentication type	Key management options	Description
Open	None	Any device can authenticate to the access point. For added security, static WEP encryption might optionally be used.
Shared Key	None	The phone encrypts the challenge text by using the WEP key and the access point must verify the WEP key that was used to encrypt the challenge text before network access is available.
LEAP or EAP-FAST	None	The RADIUS server authenticates the username and password before network access is available. For more information about name and password authentication, see Wireless Setup menu, on page 108.
Auto (AKM)	WPA, WPA2, or CCKM	The phone looks for an access point with one of the key management options enabled. The username and password are authenticated by the RADIUS server before network access is available.
Auto (AKM)	WPA-Pre-shared key, WPA2-Pre-shared key	The phone looks for an access point that has one of the key management options enabled. Authentication uses the configured WPA-Pre-shared key or WPA2-Pre-shared key

For more information, see Authentication Methods, on page 94.

4 Load the stored phone image. The Cisco Unified IP Phone has nonvolatile flash memory in which the phone stores firmware images and user-defined preferences. At startup, the phone runs a bootstrap loader that loads a phone firmware image that is stored in flash memory. Using this image, the phone initializes the software and hardware.

   For more information, see Startup Problems, on page 267.

5 Configure the VLAN. If the Cisco Unified IP Phone is connected to a Cisco Catalyst switch, the switch next informs the phone of the voice VLAN that is defined on the switch. The phone needs to know the VLAN membership before it can proceed with the Dynamic Host Configuration Protocol (DHCP) request for an IP address.

   For more information, see Ethernet Setup menu, on page 104 and Startup Problems, on page 267.

6 Obtain an IP address. If the Cisco Unified IP Phone is using DHCP to obtain an IP address, the phone queries the DHCP server to obtain one. If you are not using DHCP in your network, you must assign static IP addresses to each phone locally.

   For more information, see Ethernet Setup menu, on page 104 and Startup Problems, on page 267.

7 Request the CTL file. The TFTP server stores the CTL file. This file contains the certificates that are necessary for establishing a secure connection between the phone and Cisco Unified Communications Manager.

   For more information, see the *Cisco Unified Communications Manager Security Guide*, "Configuring the Cisco CTL Client" chapter.

8 Request the ITL file. The phone requests the ITL file after it requests the CTL file. The ITL file contains the certificates of the entities that the phone can trust. The certificates are used to authenticate a secure connection with the servers or to authenticate a digital signature signed by the servers. Cisco Unified Communications Manager 8.5 and later supports the ITL file.

   For more information, see Cisco Unified IP Phone and telephony networks, on page 41 and Troubleshooting and Maintenance, on page 267 chapter.

9 Access a TFTP server. In addition to assigning an IP address, the DHCP server directs the Cisco Unified IP Phone to a TFTP Server. If the phone has a statically defined IP address, you must configure the TFTP server locally on the phone; the phone then contacts the TFTP server directly.

Note You can also assign an alternate TFTP server to use instead of the one that DHCP assigns.

   For more information, see Ethernet Setup menu, on page 104 and Startup Problems, on page 267.

10 Request the configuration file. The TFTP server has configuration files, which define parameters for connecting to Cisco Unified Communications Manager and other information for the phone.

   For more information, see Cisco Unified Communications Manager Phone Addition Methods, on page 50 and Startup Problems, on page 267.

11 Contact Cisco Unified Communications Manager. The configuration file defines how the Cisco Unified IP Phone communicates with Cisco Unified CM and provides a phone with the load ID. After it obtains the file from the TFTP server, the phone attempts to make a connection to the highest priority Cisco Unified CM on the list.

If the security profile of the phone is configured for secure signaling (encrypted or authenticated) and the Cisco Unified Communications Manager is set to secure mode, the phone makes a TLS connection. Otherwise, the phone makes a nonsecure TCP connection.

If the phone was manually added to the database, Cisco Unified Communications Manager identifies the phone. If the phone was not manually added to the database and autoregistration is enabled in Cisco Unified Communications Manager, the phone attempts to autoregister itself in the Cisco Unified Communications Manager database.

Note Autoregistration is disabled when you configure the CTL client. In this case, you must add the phone to the Cisco Unified Communications Manager database manually.

For more information, see the "Cisco Unified IP Phone and your network" chapter and the "Troubleshooting and maintenance" chapter.

Cisco Unified Communications Manager Phone Addition Methods

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

The following table provides an overview of the methods for adding phones to the Cisco Unified Communications Manager database.

Table 8: Methods for Adding Phones to the Cisco Unified Communications Manager Database

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

Autoregistration Phone Addition

By enabling autoregistration before you begin installing phones, you can:

- Add phones without first gathering MAC addresses from the phones.
- Automatically add a Cisco Unified 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.

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

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 as described in *Cisco Unified Communications Manager Security Guide*. For information about enabling autoregistration, see the "Enabling Autoregistration" section in the *Cisco Unified Communications Manager Administration Guide*.

Autoregistration and TAPS Phone Addition

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.

Note 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.

Autoregistration must be enabled in Cisco Unified Communications Manager Administration (**System** > **Cisco Unified CM**) for TAPS to function.

Note When you configure the cluster for mixed mode through the Cisco CTL client, autoregistration is automatically disabled. When you configure the cluster for nonsecure mode through the Cisco CTL client, autoregistration is not enabled automatically.

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

Cisco Unified Communications Manager Administration Phone Addition

You can add phones individually to the Cisco Unified Communications Manager database by using Cisco Unified Communications Manager Administration. To do so, you first need to obtain the MAC address for each phone.

After you collect MAC addresses, in Cisco Unified Communications Manager Administration, choose **Device** > **Phone** and click **Add New** to begin.

For complete instructions and conceptual information about Cisco Unified Communications Manager, see the "Cisco Unified Communications Manager Overview" chapter in the *Cisco Unified Communications Manager System Guide*.

Add Phones using 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 detailed instructions about adding phones through the Bulk Administration menu, see the *Cisco Unified Communications Manager Bulk Administration Guide*, "Inserting Phones" chapter.

For more information about using BAT, see the *Cisco Unified Communications Manager Bulk Administration Guide*. For more information about creating of BAT Phone Templates, see the "Phone Template" section in the *Cisco Unified Communications Manager Bulk Administration Guide*.

To add a phone to the Cisco Unified Communications Manager, follow these steps:

Procedure

Step 1 From Cisco Unified Communications Manager, 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, Device Security Profile, and so on.

Step 5 Click **Save**.

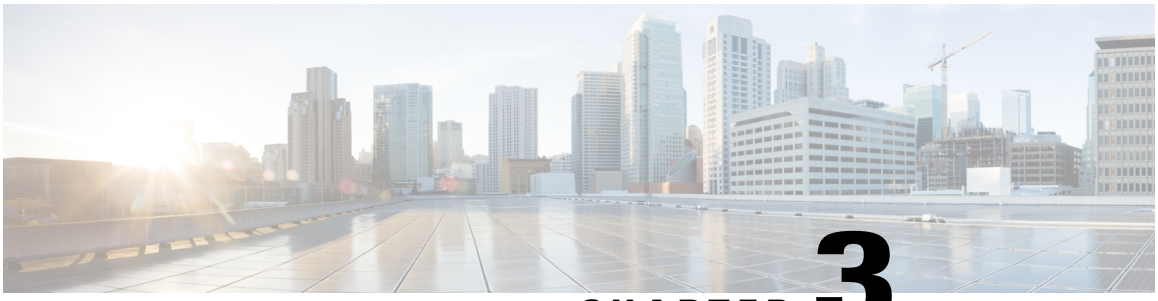
Step 6 From Cisco Unified Communications Manager, choose **Device** > **Phone** > **Add New** to add a phone by using an existing BAT phone template.

Cisco Unified IP Phone MAC Address Determination

This manual describes several procedures that require you to determine the MAC address of a Cisco Unified IP Phone. You can determine the MAC address of a phone in these ways:

- From the phone, press **Applications**, choose **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 the **Device Information** hyperlink.



CHAPTER 3

Cisco Unified IP Phone Installation

This chapter helps you install the Cisco Unified IP Phone on an IP telephony network.

Note Before you install a Cisco Unified IP Phone, you must decide how to configure the phone in your network. Then you can install the phone and verify functionality. For more information, see Cisco Unified IP Phone and telephony networks, on page 41.

This chapter contains the following topics:

Before You Begin

Before installing the Cisco Unified IP Phone, review the following sections.

Network Requirements

For the Cisco Unified IP Phone to successfully operate as a Cisco Unified IP Phone endpoint in your network, your network must meet the following requirements:

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

- IP network that supports DHCP or manual assignment of IP address, gateway, and subnet mask

Note The Cisco Unified IP 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.

- Voice over Wireless LAN (Optional for Cisco Unified IP Phone 9971)
  - Cisco Aironet Access Points (APs) are configured to support Voice over WLAN (VoWLAN).
  - Controllers and switches are configured to support VoWLAN.
  - Security is implemented for authenticating wireless voice devices and users.

Cisco Unified Communications Manager

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

If you plan to use autoregistration, verify that autoregistration is enabled and is properly configured in Cisco Unified Communications Manager Administration before you connect any Cisco Unified IP Phone to the network. For information about enabling and configuring autoregistration, see the *Cisco Unified Communications Manager Administration Guide*.

You must use Cisco Unified Communications Manager Administration to configure and assign telephony features to the Cisco Unified IP Phones.

In Cisco Unified Communications Manager Administration, you can add users to the database and associate them with specific phones. In this way, users gain access their Cisco Unified Communications Manager User Options page to configure items such as call forwarding, speed dialing, and voice messaging system options.

Related Topics

Cisco Unified Communications Manager Phone Addition Methods, on page 50
Telephony features available for Cisco Unified IP Phone, on page 130
Add Users to Cisco Unified Communications Manager, on page 181

Cisco Unified IP Phone Components

The Cisco Unified IP Phone includes components on the phone or as accessories for the phone.

Network and Computer Ports

The back of the Cisco Unified IP Phone includes these ports:

- Network port

- Computer port

Each port supports 10/100/1000 Mbps half- or full-duplex (except for full-duplex only for 1000 Mbps) connections to external devices. You can use Category 3, 5, or 5e cabling for 10 Mbps connections, Category 5 or 5e for 100 Mbps connections, and Category 5e for 1000 Mbps connections.

Use the SW network port to connect the phone to the network. You must use a straight-through cable on this port. The phone can also obtain inline power from a switch over this connection.

Use the computer port to connect a network device, such as a computer, to the phone. You must use a straight-through cable on this port.

Handset

The wideband-capable handset is designed especially for use with a Cisco Unified IP Phone. The handset includes a light strip that indicates incoming calls and voice messages that are waiting.

To connect a handset to the Cisco Unified IP Phone, plug the cable into the handset and into the Handset port on the back of the phone.

With a wall-mounted phone, you might need to adjust the handset rest to ensure that the receiver cannot slip out of the cradle.

Related Topics

Adjust Handset Rest, on page 324

Disable Speakerphone

By default, the wideband-capable speakerphone is enabled on the Cisco Unified IP Phone.

You can use Cisco Unified Communications Manager Administration to disable the speakerphone.

Procedure

Step 1 Access Cisco Unified Communications Manager Administration.

Step 2 Choose **Device** > **Phone** and locate the phone that you want to modify.

Step 3 In the Phone Configuration window for the phone, check the **Disable Speakerphone** check box.

Cisco Unified IP Phone 8961, 9951, and 9971 Accessory Support

The following table lists the accessories that the Cisco Unified IP Phone 8961, 9951, and 9971 supports. An “X” indicates support for a particular phone model and a dash (-) indicates no support.

Table 9: Accessory Support for the Cisco Unified IP Phone 8961, 9951, and 9971

Accessory	Type	Cisco Unified IP Phone 8961	Cisco Unified IP Phone 9951	Cisco Unified IP Phone 9971
Cisco Accessory				
Cisco Unified IP Color Key Expansion Module: See Cisco Unified IP Color Key Expansion Module Setup, on page 71	Add-on module	1	Up to 2	Up to 3
Cisco Unified Video Camera: See Cisco Unified Video Camera setup, on page 79.	Add-on module	-	X	X
Third-Party accessories				
Headsets: See Headsets, on page 59. This section includes information about each headset type.	Analog	X	X	X
	Analog Wideband	X	X	X
	Bluetooth	-	X	X
	USB (wired or wireless)	X	X	X
Microphone: See External Speakers and Microphone, on page 59.	External PC	-	X	X
Speakers: See External Speakers and Microphone, on page 59.	External PC	-	X	X

USB Port Information

The Cisco Unified IP Phone supports a maximum of five devices that connect to each USB port. Each device that connects to the phone is included in the maximum device count. For example, your phone can support five USB devices (such as three Cisco Unified IP Color Key Expansion modules, one hub, and one other standard USB device) on the side port and five additional standard USB devices on the back port. The Cisco Unified IP Phone 8961 does not contain a back USB port. Many third-party USB products count as multiple USB devices; for example, a device containing a USB hub and headset can count as two USB devices. For more information, see the USB device documentation.

Note

- Unpowered hubs are not supported, and powered hubs with more than four ports are not supported.
- USB headsets that connect to the phone through a USB hub are not supported.
- The Cisco Unified Video Camera that connects to the phone through a USB hub is not supported.

External Speakers and Microphone

External speakers and microphones are plug-and-play accessories. You can connect an external PC-type microphone and powered speakers (with amplifier) on the Cisco Unified IP Phone 9951 or 9971 by using the line in/out jacks. Connecting an external microphone disables the internal microphone and connecting an external speaker disables the internal phone speaker.

Note Using poor quality external audio devices, playing loudspeakers at very loud volumes, or placing the microphone very close to the loudspeaker may result in undesirable echo for other parties on your speakerphone calls.

Headsets

Although Cisco Systems performs internal testing of third-party headsets for use with Cisco Unified IP Phones, Cisco does not certify nor support products from headset or handset vendors.

The phone reduces some background noise that a headset microphone detects, but if you want to further reduce the background noise and improve the overall audio quality, use a noise cancelling headset.

Cisco recommends the use of good quality external devices, for example, headsets that are screened against unwanted radio frequency (RF) and audio frequency (AF) signals. Depending on the quality of headsets and their proximity to other devices, such as mobile (cell) phones and two-way radios, some audio noise or echo may still occur. Either the remote party or both the remote party and the Cisco Unified IP Phone user may hear an audible hum or buzz. A range of outside sources can cause humming or buzzing sounds; for example, electric lights, electric motors, or large PC monitors.

Note In some cases, using a local power cube or power injector may reduce or eliminate hum.

These environmental and hardware inconsistencies in the locations where Cisco Unified IP Phones are deployed mean that no single headset solution is optimal for all environments.

Cisco recommends that customers test headsets in the intended environment to determine performance before making a purchasing decision and deploying on a large scale.

Related Topics

External device use, on page 65

Audio Quality

Beyond physical, mechanical, and technical performance, the audio portion of a headset must sound good to the user and to the party on the far end. Sound quality is subjective and Cisco cannot guarantee the performance of any headsets. However, a variety of headsets from leading headset manufacturers are reported to perform well with Cisco Unified IP Phones.

For additional information, see the Headsets for Cisco Unified IP Phones and Desktop Clients page on Cisco.com.

Wired Headsets

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

Related Topics

Analog Headsets, on page 61

Connect to Wired Headset

To connect a wired headset to the Cisco Unified IP Phone, perform these steps:

Procedure

Step 1 Plug the headset into the Headset port on the back of the phone.

Step 2 Press the **Headset** button on the phone to place and answer calls using the headset.

Disable Wired Headset

You can disable the headset by using Cisco Unified Communications Manager Administration. If you do so, you also disable the speakerphone.

Procedure

Step 1 To disable the headset from Cisco Unified Communications Manager Administration, choose **Device** > **Phone** and locate the phone that you want to modify.

Step 2 In the Phone Configuration window (Product Specific Configuration layout portion), select the **Disable Speakerphone and Headset** check box.

USB Headsets

Wired and wireless USB headsets are supported. You can connect a USB headset (or the base station for a wireless headset) to either the back USB port (if your phone has this port) or to the side USB port.

The Cisco Unified IP Phone 9951 and 9971 contains both a back USB port and a side USB port, while the Cisco Unified IP Phone 8961 contains only a side USB port.

Related Topics

Wireless Headsets, on page 62

USB headset enabling

You must enable the applicable USB port (either the back USB port parameter or the side USB port parameter) in Cisco Unified Communications Manager Administration (in the Product Specific Configuration layout portion of the window). Also, for the Enable/Disable USB Classes parameter in Cisco Unified Communications Manager Administration, ensure that **Audio Class** is selected.

These parameters can be enabled on either the Phone Configuration window (**Device** > **Phone**), the Enterprise Phone Configuration window (**System** > **Enterprise Phone Configuration**), or the Common Phone Profile window (**Device** > **Device Settings** > **Common Phone Profile**). Also check the corresponding Override Common Settings parameter in the configuration window.

Related Topics

Product-Specific Configuration, on page 165

USB Headset Disabling

To disable the USB headset, disable the USB port (or disable the Audio Class parameter) that you enabled in Cisco Unified Communications Manager Administration. Also, you can select another type of headset in the Accessories window on the phone, thus disabling the previously enabled headset.

Analog Headsets

Analog headsets are supported on the Cisco Unified IP Phone 8961, 9951, and 9971. However, the Cisco Unified IP Phone 8961, 9951, and 9971 cannot detect when an analog headset is plugged in. For this reason, the analog headset displays by default in the Accessories window on the phone screen.

Displaying the analog headset as the default allows users to enable wideband for the analog headset.

Enable Wideband on Analog Headsets

The phone is unable to detect whether the headset supports the wideband codec, but the user can enable wideband on analog headsets by following these steps:

Procedure

Step 1 On the Cisco Unified IP Phone, press **Applications** .

Step 2 Select **Accessories**.

Step 3 Highlight the analog headset, then press **Setup**.

Step 4 Turn wideband on or off for the selected headset by using the on/off toggle.

Enable Wideband Codec on Analog Headsets

If the wideband on/off toggle is not enabled, follow these steps to ensure that the user can enable wideband codec on an analog headset:

Procedure

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

Step 2 In the Find and List Phones window, enter the search criteria for the phone to which you want to add the analog headset, then click **Find**.

Step 3 Click on the Device Name that you want. The Phone Configuration window displays.

Step 4 On the Product Specific Configuration Layout portion of the Phone Configuration window, ensure that the Wideband Headset UI Control option is enabled. (This option is enabled by default.)

Step 5 In the Product Specific Configuration Layout portion of the Phone Configuration window, you can also set the Wideband Headset option. (This option is also enabled by default).

Wireless Headsets

You can use a wireless headset with the Cisco Unified IP Phone.

Find Information on Supported Wireless Headsets

The Cisco website provides information about wireless headsets that work with your IP phone.

Procedure

Step 1 Go to the following URL:
http://www.cisco.com/en/US/partner/prod/voicesw/ucphone_headsets.html

Step 2 See the wireless headset documentation for information about connecting the headset and using the features.

Bluetooth Wireless Headsets

The Cisco Unified IP Phone 9951 and 9971 supports Bluetooth Class 2 technology for headsets that support Bluetooth. Bluetooth enables low-bandwidth wireless connections within a range of 30 feet (10 meters). The best performance is in the 3- to 6-foot range (1 to 2 meters). You can pair up to 5 headsets, but only the last headset that was connected is used as the default.

Potential interference issues can occur. Cisco recommends that you reduce the proximity of other 802.11b/g devices, Bluetooth devices, microwave ovens, and large metal objects. If possible, configure other 802.11 devices to use the 802.11a channels.

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

Bluetooth Wireless Headset and Cisco Unified IP Phones

The Cisco Unified IP Phones 9951 and 9971 support Bluetooth wireless headsets.

The Cisco Unified IP Phone uses a shared key authentication and encryption method to connect with headsets. The Cisco Unified IP Phone can connect with up to five headsets at a time. The last connected headset is used as the default. Pairing is typically performed once for each headset.

After a device is paired, the Bluetooth connection is maintained as long as both devices (phone and headset) are enabled and within range of each other. The connection typically reestablishes itself automatically if either of the devices powers down then powers up. However, some headsets require user action to reestablish the connection.

The Bluetooth icon  indicates whether a device is connected.

When headsets are more than 30 feet (10 meters) away from the Cisco Unified IP Phone, Bluetooth drops the connection after a 15- to 20-second timeout. If the paired headset comes back into range of the Cisco Unified IP Phone and the phone is not connected to another Bluetooth headset, the in-range Bluetooth headset automatically reconnects. For certain phone types that operate in power-save modes, the user can *wake up* the headset by tapping on the operational button to initiate the reconnect.

You must enable the headset and then add it as a phone accessory.

Handsfree Profile

Your phone supports various Handsfree Profile features that enable you to use hands-free devices (such as Bluetooth wireless headsets) to perform certain tasks without having to handle the phone. For example, instead of pressing Redial on the phone, users can redial a number from their Bluetooth wireless headset by following instructions from the headset manufacturer.

These hands-free features apply to Bluetooth wireless headsets that are used with the Cisco Unified IP Phone 9951 and 9971:

- Answer a call
- End a call
- Change the headset volume for a call
- Redial
- Caller ID

- Reject
- Divert
- Hold and Accept
- Release and Accept

Hands-free devices may differ as to how features are activated. Device manufacturers may also use different terms when referring to the same feature.

For more information, see the manufacturer documentation.

Add Headset as Phone Accessory

After the Bluetooth wireless headset is enabled through Cisco Unified Communications Manager Administration, you must add the headset as an accessory to the phone.

Procedure

Step 1 On the Cisco Unified IP Phone 9951 or 9971, press **Applications** and select **Accessories**.

Step 2 Select **Add Bluetooth Accessory**.
The Adding Bluetooth Accessory window appears. A message tells you to make sure your accessory is discoverable, which means that the Bluetooth should be powered on and in discoverable or pairing mode.

After the Bluetooth device is located, the name appears in the window, and a message asks for a PIN so that the Bluetooth device can be paired with the Cisco Unified IP Phone.

Step 3 The Cisco Unified IP Phone automatically tries to pair with the headset by using a PIN of "0000." If the headset uses a different PIN, enter the correct PIN by referring to the user guide that came with the headset.

Note Cisco recommends that users read the headset user guide for more information about pairing and connecting the headsets.

After the phone has the correct PIN, the phone tries to connect to the accessory. The phone provides feedback to the user while it tries to connect the accessory. If unable to connect, an error alert appears to let the user know the reason for the failure. A timeout of 10 seconds allows the phone to try to connect the accessory. If the timer expires without a successful connection, an error alert displays.

Enable Bluetooth Wireless Headset

Before you use your Bluetooth Wireless headset, you must enable it.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Device** > **Phone**, locate the phone you want to modify, and go to the Phone Configuration window for that phone.

Step 2 In the Phone Configuration window, select **Enable** for the Bluetooth setting and **Handsfree** for the Bluetooth Profiles setting.

Step 3 Save your changes.

Remove Bluetooth Device from Phone

When you want to remove a Bluetooth device, you delete it from the Accessories menu.

Procedure

Step 1 Press **Applications** .

Step 2 Select **Accessories**.

Step 3 Highlight the device that you want to remove and press **Delete**.

Related Bluetooth documentation

For information about how to use your Bluetooth wireless headset, see:

- *Cisco Unified IP Phone 8961, 9951, and 9971 User Guide for Cisco Unified Communications Manager (SIP)*
- User guides provided with your headset

Important Note About Headset Types

Only one headset type works at any given time, so if you use both a Bluetooth headset and an analog headset that are attached to the phone, enabling the Bluetooth headset disables the analog headset. To enable the analog headset, disable the Bluetooth headset. Plugging a USB headset into a phone that has Bluetooth headset enabled disables both the Bluetooth and analog headset. If you unplug the USB headset, you can either enable the Bluetooth headset or disable the Bluetooth headset to use the analog headset.

External device use

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

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

- Move the external device away from the source of the RF or AF signals.
- Route the external device cables away from the source of the RF or AF signals.
- Use shielded cables for the external device, or use cables with a better shield and connector.
- Shorten the length of the external device cable.
- Apply ferrites or other such devices on the cables for the external device.

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

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

Install Cisco Unified IP Phone

You must connect the Cisco Unified IP Phone to the network and to a power source before using it. For information on connecting the phone, see the figures in Cisco Unified IP Phone 8961, 9951, and 9971, on page 2.

Note Before you install a phone, even if it is new, upgrade the phone to the current firmware image.

Before using external devices, read External device use, on page 65 for safety and performance information.

Note Firmware upgrades over the WLAN interface may take longer than upgrading over the wired interface, depending on the quality and bandwidth of the wireless connection. Some upgrades may take more than hour.

To install a Cisco Unified IP Phone, perform the tasks described in the following steps.

Procedure

Step 1 Connect the handset to the handset port.

Step 2 Connect a headset to the headset port. You can add a headset later if you do not connect one now. For more information, see Headsets, on page 59.

Step 3 Connect a wireless headset (for the Cisco Unified IP Phone 9951 and 9971 only). You can add a wireless headset later if you do not want to connect one now. For more information, see your wireless headset documentation.

Step 4 Connect a straight-through Ethernet cable from the switch to the network port labeled 10/100/1000 SW on the Cisco Unified IP Phone. Each Cisco Unified IP Phone ships with one Ethernet cable in the box. Use Category 3, 5, or 5e cabling for 10 Mbps connections; Category 5 or 5e for 100 Mbps connections; and Category 5e for 1000 Mbps connections. For more information, see Network and Computer Ports, on page 56 for guidelines.

Step 5 Connect a straight-through Ethernet cable from another network device, such as a desktop computer, to the computer port on the Cisco Unified IP Phone. You can connect another network device later if you do not connect one now.
You can use Category 3, 5, or 5e cabling for 10 Mbps connections; Category 5 or 5e for 100 Mbps connections; and Category 5e for 1000 Mbps connections. For more information, see Network and Computer Ports, on page 56 for guidelines.

Step 6 Enable the phone to use the wireless local area network (WLAN).

Note You must disconnect all Ethernet connections if you deploy the Cisco Unified IP Phone 9971 on a wireless LAN.

Step 7 Adjust the footstand. For more information, see Connect Footstand, on page 19.

Step 8 Secure the phone with a cable lock. For more information, see Phone and Cable Lock, on page 20.

Related Topics

Cisco Unified IP Phone 8961, 9951, and 9971, on page 2
Phone Startup Verification, on page 68
Network Settings, on page 68

Phone wall mount

You can mount the Cisco Unified IP Phone on the wall by using special brackets that are available in a Cisco Unified IP Phone wall mount kit. Wall mount kits must be ordered separately from the phone.

Related Topics

Cisco Unified IP Phone Wall Mount, on page 313
Cisco Unified IP Phone Non-Lockable Wall Mount, on page 325

Phone Startup Verification

After the Cisco Unified IP Phone has power connected to it, the phone begins the startup diagnostic process, by cycling through the following steps.

1. The Feature and Sessions buttons flash amber and then green in sequence during the various stages of bootup as the phone checks the hardware.
2. The main screen displays `Registering to Cisco Unified Communications Manager`.

If the phone completes these stages successfully, it has started up properly and the **Select** button stays lit until it is selected.

Network Settings

If you are not using DHCP in your network, you must configure these network settings on the Cisco Unified IP Phone after you install the phone on the network:

- IP address
- IP subnet information
- IPv6 addresses
- TFTP server IP address

If necessary, you may also configure the domain name and the DNS server settings.

Cisco Unified IP Phone Security

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 Unified 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 related topics and the *Cisco Unified Communications Manager Security Guide*.

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.

Set Up Locally Significant Certificate

Use this procedure to configure an LSC on the phone.

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.

See the *Cisco Unified Communications Manager Security Guide* for more information.

Procedure

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

Step 2 From the phone, press **Applications** and choose **Administrator Settings** > **Security Setup**.

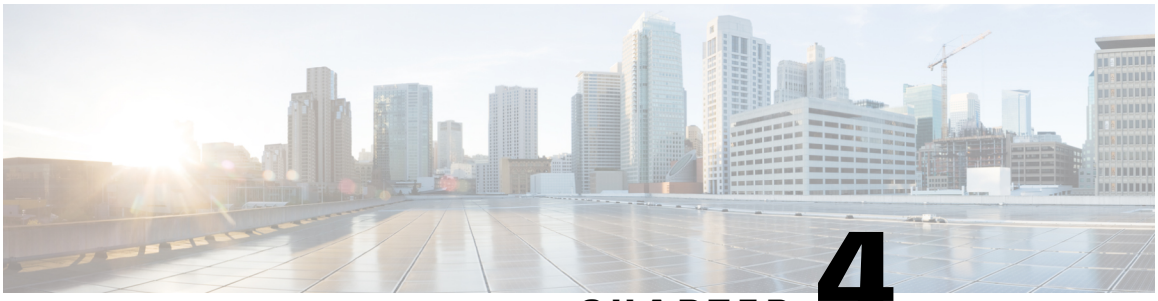
Note You can control access to the Settings menu by using the Settings Access field in the Cisco Unified Communications Manager Administration Phone Configuration window. For more information, see the *Cisco Unified Communications Manager Administration Guide*.

Step 3 Choose **LSC** and press **Select** or **Update**.
The phone prompts for an authentication string.

Step 4 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. You can stop the process at any time by pressing the **Stop** softkey from the Security Setup menu.

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 may not enabled for upgrading. If the CAPF operation deletes the LSC, the phone displays `Not Installed` to indicate that the operation succeeded. See the error messages that were generated on the CAPF server and take appropriate actions.



CHAPTER 4

Cisco Unified IP Color Key Expansion Module Setup

The Cisco Unified IP Color Key Expansion Module (KEM) attaches to your Cisco Unified IP Phone 8961, 9951, and 9971 to add additional line appearances, speed dials, or programmable buttons to your phone. The programmable buttons can be set up as phone line buttons, speed-dial buttons, or phone feature buttons.

Most call functions, such as answering a call, placing a call on hold, and transferring a call, can be performed with the Cisco Unified IP Color Key Expansion Module.

The following table lists the Cisco Unified IP Phones and the number of Key Expansion Modules that each model supports.

Note For information about installing a wall mount kit for a phone that includes a Cisco Unified IP Color Key Expansion Module, see Wall Mount Components for Phone with Key Expansion Module, on page 318.

Table 10: Cisco Unified IP Phones and Supported KEMs

Cisco Unified IP Phone model	Supported KEMs
9971	3 KEMs with 108 lines or buttons
9951	2 KEMs with 72 lines or buttons
8961	1 KEM with 36 lines or buttons

This chapter includes the following topics:

- Key Expansion Module Removal, page 76
- Troubleshoot the KEM, page 76

Key Expansion Module Installation on Cisco Unified IP Phone

This section describes the requirements and steps to install a Cisco Unified IP Phone Key Expansion Module.

KEM Power Information

The Cisco Unified IP Color Key Expansion Module for the Cisco Unified IP Phone 8961, 9951, and 9971 possesses the following power consumption and power scheme:

Power consumption

48V DC, 5W per KEM

Power scheme

- If the Cisco Unified IP Phone 8961, 9951, and 9971 uses AT PoE, at least one KEM can be powered up.
- If the phone uses a power adapter, three KEMs can be powered up for the Cisco Unified IP Phone 9971, two KEMs can be powered up for the Cisco Unified IP Phone 9951, and one KEM can be powered up for the Cisco Unified IP Phone 8961.
- If the Cisco Unified IP Phone 8961, 9951, and 9971 uses AF PoE, a KEM cannot be powered up.
- With AT power, the Cisco Unified IP Phones 9951 and 9971 can support two KEMs plus a USB headset or another USB device that is independently powered and only uses USB for signalling.
- The Cisco Unified IP Phone 9971 needs a power cube to support three KEMS.
- With AF power, the Cisco Unified IP Phones 9951 and 9971 need power cubes for any KEMS. The Cisco Unified IP Phone 8961 can support one KEM with CDP, AF power, and no power cube.

Connect Single KEM to Cisco Unified IP Phone

To connect a single KEM to the Cisco Unified IP Phone, follow these steps:

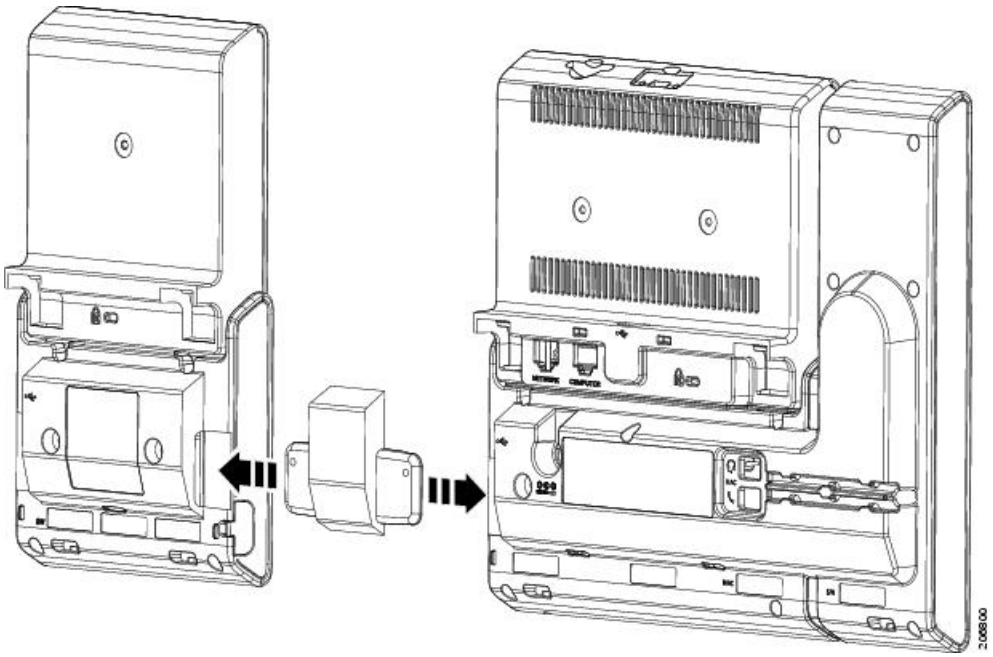
Procedure

Step 1 Position the phone so that the front of the phone is facing up.

Step 2 Connect one end of the KEM spine connector to the accessory connector on the Cisco Unified IP Phone.

Step 3 Connect the other end of the KEM spine connector to the KEM as shown in the following figure.

Figure 1: Connecting the KEM Spine Connector to the Cisco Unified IP Phone and KEM



Step 4 Fasten the screws on the spine connector after connecting both the ends.

Note You can use a coin or screwdriver to fasten the screws. Make sure that the sides of the screw heads are fully inserted into the spine connector cavity and tightened.

Connect Two or More KEMs to Phone Using KEM Spine Connector

To connect two or more KEMs to the Cisco Unified IP Phone, follow these steps:

Procedure

Step 1 Position the phone so that the front of the phone is facing up.

Step 2 Connect one end of the KEM spine connector to the accessory connector on the Cisco Unified IP Phone and the other end of the spine connector to a KEM, as seen in Connect Single KEM to Cisco Unified IP Phone, on page 72. The first KEM is now connected to the Cisco Unified IP Phone.

Step 3 Use a second KEM spine connector to connect the second KEM to the first KEM.

Step 4 Use a third KEM spine connector to connect the third KEM to the second (middle) KEM. The following figure shows a Cisco Unified IP Phone with three KEMs attached.

Figure 2: Cisco Unified IP Phone with Three KEMs Attached

Step 5 Fasten the screws on the spine connectors after connecting both the ends.

Set up Key Expansion Module in Cisco Unified Communications Manager Administration

To configure the Cisco Unified IP Color Key Expansion Module on the Cisco Unified IP Phone, follow these steps:

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Device** > **Phone**.
The Find and List Phones window appears. You can search for one or more phones that you want to configure for the Cisco Unified IP Color Key Expansion Module.

Step 2 Select and enter your search criteria and click **Find**.
The Find and List Phones window appears with a list of phones that match your search criteria.

Step 3 Click the IP phone that you want to configure for the Cisco Unified IP Color Key Expansion Module. The Phone Configuration window appears.

Step 4 Scroll down to the Expansion Module Information section on the right pane of the Phone Configuration window, and choose the appropriate expansion module (or "none") for the Module 1, Module 2 and Module 3 fields, in that order.
For the Module Load Name, enter the custom software for the appropriate expansion module, if applicable. The value that you enter overrides the default value for the current model. Ensure that the firmware load matches the module load. If the Module Load Name is left blank, the default load (the load bundled with the phone load) is installed.

For the number of supported KEMs per phone model, see Cisco Unified IP Color Key Expansion Module Setup, on page 71.

Step 5 Ensure that the Side USB Port parameter is enabled.

Note If the Side USB Port is disabled, the KEM does not work.

Step 6 Be sure to select the phone button template (in the Device Information portion of the Phone Configuration window) that is configured to make full use of the KEMs attached to the phone.

Step 7 Click **Save**.

Key Expansion Module Settings on Phone

After you install one or more KEMs on the phone and configure them in Cisco Unified Communications Manager Administration, the KEMs are automatically recognized by the Cisco Unified IP Phone 8961, 9951, and 9971.

When multiple KEMs are attached, they are numbered according to the order in which they connect to the phone. For example (see Connect Two or More KEMs to Phone Using KEM Spine Connector, on page 73):

- Key Expansion Module 1 is the KEM closest to the phone.
- Key Expansion Module 2 is the KEM in the middle.
- Key Expansion Module 3 is the KEM farthest to the right.

You can select a KEM, and then choose one of the following softkeys:

- Exit: Returns to the Applications menu.
- Details: Provides details about the selected KEM.
- Setup: Allows you to configure the brightness of the selected KEM. This can also be done using the Preferences menu. For details, see the *Cisco Unified IP Phone 8961, 9951, and 9971 User Guide for Cisco Unified Communications Manager (SIP)*, "Accessories" chapter, "Adjust brightness" section.

Access the Key Expansion Module Setup

Procedure

On the phone, press **Applications** and then press **Accessories**. All properly installed and configured KEMs display in the list of accessories.

Upgrade the Key Expansion Module

To automatically upgrade KEMs to the latest load, follow these steps:

Procedure

Step 1 Power on the KEM, press **Page 1**, and do not release the key. When the LCD turns white, continue pressing **Page 1** for at least one second.

Step 2 Release **Page 1**; LEDs should turn red. Immediately press **Page 2** and continue pressing **Page 2** for at least one second.

Step 3 Release **Page 2**; all LEDs should turn amber.

Step 4 Press Lines **5**, **14**, **1**, **18**, **10**, and **9** in sequence.
The LCD should turn blue, and the spinning loader icon displays in the center.

The KEM starts to upgrade.

Key Expansion Module Removal

If you need to remove all existing KEMs from the phone, detach them from the phone, then go to Cisco Unified Communications Manager Administration and update the phone configuration file accordingly.

If you are removing one or more KEMs but still leaving one or more KEMs attached to the phone, see Key Expansion Module Installation on Cisco Unified IP Phone, on page 72 for instructions on how to connect the KEMs and phone based on how many KEMs remain. Also, go to Cisco Unified Communications Manager Administration and update the phone configuration file accordingly.

Troubleshoot the KEM

To obtain KEM troubleshooting information, follow these steps:

Procedure

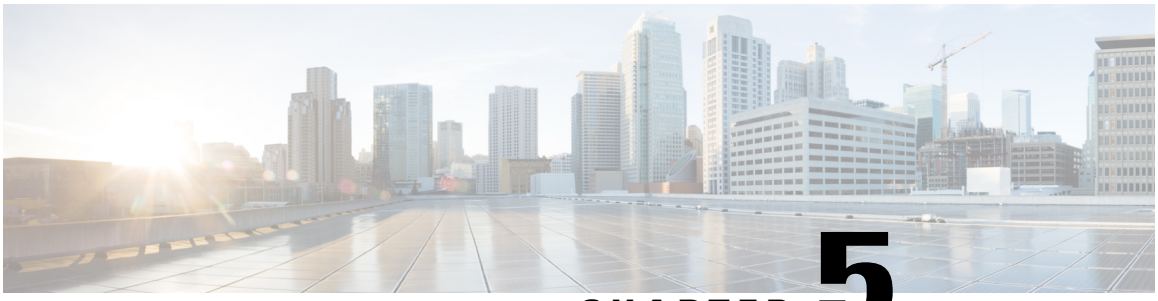
Step 1 Open a CLI.

Step 2 Enter the following command to enter debug mode:
debugsh

Step 3 Enter **?** to see all available commands and options.

Step 4 Use the applicable commands and options to find the desired KEM information.

Step 5 To exit debug mode, press **Ctrl-C**.



CHAPTER 5

Cisco Unified Video Camera setup

The Cisco Unified IP Phone 9951 and 9971 supports the add-on Cisco Unified Video Camera accessory.

The Cisco Unified Video Camera connects to your Cisco Unified IP Phone and allows you to make a point-to-point video call with another Cisco Unified IP Phone with a Cisco Unified Video Camera attached. If a Cisco Unified Video Camera is not attached to the phone, the phone can only receive one-way video.

Note The Cisco Unified IP Phone 8961 does not support the Cisco Unified Video Camera and does not display video.

This chapter contains the following information:

Set up Cisco Unified Video Camera

To configure the Cisco Unified Video Camera, you must perform the following configuration steps in Cisco Unified Communications Manager Administration.

You can enable the parameters that are described in the following procedure in one of the following windows:

- Phone Configuration window **(Device** > **Phone)**
- Enterprise Phone Configuration window (**System** > **Enterprise Phone Configuration**)
- Common Phone Profile window (**Device** > **Device Settings** > **Common Phone Profile**)

Be sure to also check the corresponding Override Common Settings parameter in the configuration window. The Phone Configuration window is used for purposes of the procedure description.

For more information about parameters that can be configured in any of these three configuration windows, see Product-Specific Configuration, on page 165.

Procedure

Step 1 In the Phone Configuration window (**Device** > **Phone**) of the phone to which you are adding the Cisco Unified Video Camera, enable the Cisco Camera parameter. This field is located in the Product Specific Configuration Layout portion of the window.

Step 2 In the same window, enable the Video Capabilities parameter.

Step 3 Click **Save**.

Cisco Unified Video Camera Attachment

To install the Cisco Unified Video Camera, you can either:

- Attach the camera to your phone.
- Attach the camera to your computer monitor (or to another object in your work area).

The USB port connector on the bottom of the Cisco Unified Video Camera attaches to the back port (not the side port) on the Cisco Unified IP Phone 9951 or 9971. As you attach the USB connector to the back port on the phone, the camera should slide easily into the camera pin holes on the phone.

Phone Connections for Cisco Unified IP Phone 9951, on page 8 shows the location of the back USB port and the camera pin holes for the Cisco Unified IP Phone 9951. Phone Connections for Cisco Unified IP Phone 9971, on page 14 shows the location of the back USB port and the camera pin holes for the Cisco Unified IP Phone 9971.

For the complete installation procedure, see the *Cisco Unified Video Camera Quick Start Guide* at this location:

http://www.cisco.com/en/US/products/ps10655/products_user_guide_list.html

Camera Settings

After you attach the camera on your phone, you can control the features of the camera.

Adjust View Area Setting

The View Area setting acts as a wide angle and zoom function for your camera and allows you to adjust the view area that is shared during video streaming.

Procedure

Step 1 On the Cisco Unified IP Phone, press **Applications**.
Step 2 Select **Accessories**.
Step 3 Highlight **Cisco Unified Camera**.
Step 4 Press **Setup**.
Step 5 Select **View Area**.
Step 6 Use the arrows on the **Navigation** pad to increase or decrease the view area.
Step 7 Press **Save**.

Adjust Brightness Setting

The Brightness setting affects the video that you transmit to others. However, it does not affect the video that you receive from other parties. You can adjust the Brightness setting to improve the quality of the video during streaming.

Note Because the field of view can affect brightness, adjust the View Area feature for your camera before adjusting the Brightness setting.

To adjust the Brightness setting, follow these steps:

Procedure

Step 1 On the Cisco Unified IP Phone, press **Applications**.
Step 2 Select **Accessories**.
Step 3 Highlight **Cisco Unified Camera**.
Step 4 Press **Setup**.
Step 5 Select **Brightness**.
Step 6 Use the arrows on the **Navigation** pad to increase or decrease brightness.
Step 7 Press **Save**.

Adjust Auto Transmit Setting

The Auto Transmit setting allows you to control the streaming of videos for both inbound and outbound calls. When Auto Transmit is on (default setting), the camera streams video automatically during calls. When Auto Transmit is off, video for each call is automatically muted (however, your phone still receives video). To

resume video transmission in this case, press the **Unmute Video** softkey. To turn the Auto Transmit setting on or off, follow these steps:

Procedure

Step 1 On the Cisco Unified IP Phone, press **Applications**.

Step 2 Select **Accessories**.

Step 3 Highlight **Cisco Unified Camera**.

Step 4 Press **Setup**.

Step 5 Move the **Auto Transmit** slider bar to **On** or **Off**.

Perform Camera Postinstallation Checks

After installing the Cisco Unified Video Camera, perform the following checks:

1 Wait until the `camera ready` message appears.

Note The camera may need to upgrade after installation. It may take a few minutes before the camera is operational.

2 Press **Video Preview** to check the picture quality.

- If the video preview image looks too blue, try increasing the camera Brightness setting.
- If the background looks washed out, try decreasing the camera Brightness setting.

Note For information about adjusting camera settings on the phone, see the *Cisco Unified Video Camera Quick Start Guide* at this location:

http://www.cisco.com/en/US/products/ps10655/products_user_guide_list.html

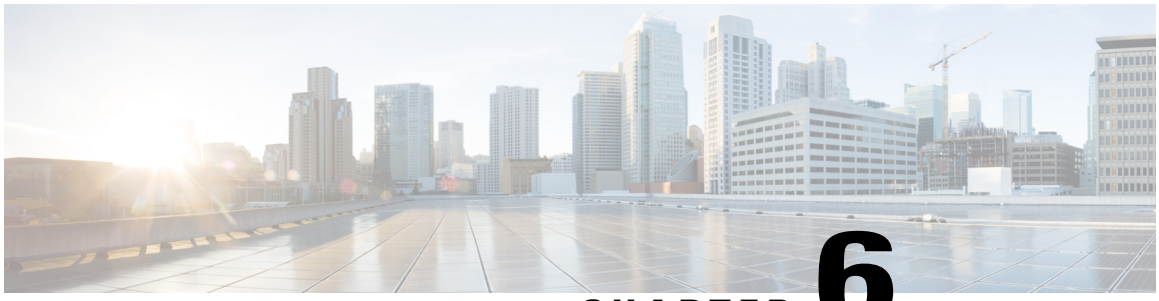
3 Move the phone and camera to a position where no bright lights are in the field of view.

4 Move the phone and camera so that the user is illuminated by light that comes from the front.

Cisco Unified Video Camera Information

For information about placing and receiving video calls, setting up video conferences, and adjusting camera settings on the phone, see the *Cisco Unified Video Camera Quick Start Guide* at this location:

http://www.cisco.com/en/US/products/ps10655/products_user_guide_list.html



CHAPTER 6

VoIP Wireless Network

This chapter provides an overview of the interaction between a wireless-capable Cisco Unified IP Phone 9971 and other key components of a VoIP network in a wireless local area network (WLAN) environment.

Note For instructions on deploying and configuring a wireless Cisco Unified IP Phone 9971, see the *Cisco Unified IP Phone 9971 Wireless LAN Deployment Guide* at this location:

http://www.cisco.com/en/US/docs/voice_ip_comm/cuipph/9971_9951_8961/7_1_3/english/deployment/guide/9971dply.pdf

This chapter contains the following sections:

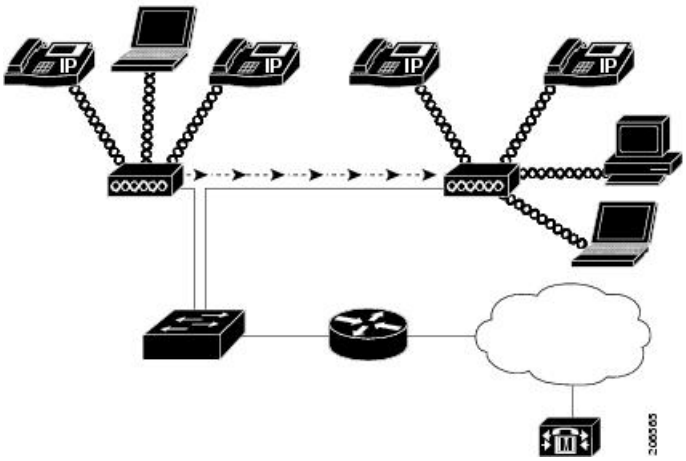
Wireless LAN

With the introduction of wireless communication, Cisco Unified IP Phones with wireless capability, such as the Cisco Unified IP Phone 9971, can provide voice communication within the corporate WLAN. The Cisco Unified IP Phone depends upon and interacts with wireless access points (AP) and key Cisco IP telephony components, including Cisco Unified Communications Manager Administration, to provide wireless voice communication. Cisco Access Points can run in standalone or unified mode. Unified mode requires the Cisco Unified Wireless LAN Controller.

The Cisco Unified IP Phone 9971 exhibits Wi-Fi capabilities which can be used with 802.11a, 802.11b, and 802.11g Wi-Fi.

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

Figure 3: WLAN with wireless IP phones



When a Cisco Unified IP Phone powers on, it searches for and becomes associated with an AP if the phone wireless access is set to On.

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

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

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

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

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

WLAN Standards and Technologies

This section describes WLAN standards and technology.

802.11 Standards for WLAN Communications

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

- 802.11a: Uses the 5 GHz band that provides more channels and improved data rates by using OFDM technology. Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) support this standard.
- 802.11b:Specifies the radio frequency (RF) of 2.4 Ghz for both transmitting and receiving data at lower data rates (1, 2, 5.5, 11 Mbps).
- 802.11d: Enables access points to advertise their currently supported radio channels and transmit power levels. The 802.11d enabled client then uses that information to determine the channels and powers to use. The Cisco Unified IP Phone 9971 requires World mode (802.11d) to determine which channels are legally allowed for any given country. For supported channels, see the following table. Ensure that 802.11d is properly configured on the Cisco IOS Access Points or Cisco Unified Wireless LAN Controller.
- 802.11e: Quality of Service (QoS)
- 802.11g:Uses the same unlicensed 2.4 Ghz band as 802.11b, but extends the data rates to provide greater performance by using Orthogonal Frequency Division Multiplexing (OFDM) technology. OFDM is a physical-layer encoding technology for transmitting signals by using RF.
- 802.11h: 5 GHz spectrum and transmit power management
- 802.11i: Security

Part number	Band range	Available channels	5 GHz channel set
CP-9971-K9	2.412 – 2.484 GHz 5.180 – 5.240 GHz 5.260 – 5.320 GHz 5. 500 – 5.700 GHz 5.745 – 5.805 GHz	13 (14 in Japan) 4 4 11 4	UNII-2 UNII-2 UNII-2 Extended UNII-3

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

Related Topics

World Mode (802.11d), on page 85

World Mode (802.11d)

If you are using the Cisco Unified IP Phone 9971 in World mode, you must enable World mode (802.11d). The Cisco Unified IP Phone 9971 uses 802.11d to determine which channels and transmit powers to use and inherits the client configuration from the associated access point.

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

Because all countries support these frequencies, you can attempt to scan these channels regardless of World mode (802.11d) support. For the countries that support 2.4GHz, see *Cisco Unified IP Phone 9971 Wireless LAN Deployment Guide* at this location:

http://www.cisco.com/en/US/products/ps10453/products_implementation_design_guides_list.html

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

You must enable World mode for Cisco Autonomous Access Points by using the following commands:

Interface dot11radio X

world-mode dot11d country US both

Supported Countries

The Cisco Unified IP Phone 9971 supports the following countries:

Argentina (AR)	India (IN)	Poland (PL)
Australia (AU)	Indonesia (ID)	Portugal (PT)
Austria (AT)	Ireland (IE)	Puerto Rico (PR)
Belgium (BE)	Israel (IL)	Romania (RO)
Brazil (BR)	Italy (IT)	Russian Federation (RU)
Bulgaria (BG)	Japan (JP)	Saudi Arabia (SA)
Canada (CA)	Korea (KR / KP)	Singapore (SG)
Chile (CL)	Latvia (LV)	Slovakia (SK)
Colombia (CO)	Liechtenstein (LI)	Slovenia (SI)
Costa Rica (CR)	Lithuania (LT)	South Africa (ZA)
Cyprus (CY)	Luxembourg (LU)	Spain (ES)
Czech Republic (CZ)	Malaysia (MY)	Sweden (SE)
Denmark (DK)	Malta (MT)	Switzerland (CH)
Estonia (EE)	Mexico (MX)	Taiwan (TW)
Finland (FI)	Monaco (MC)	Thailand (TH)
France (FR)	Netherlands (NL)	Turkey (TR)
Germany (DE)	New Zealand (NZ)	Ukraine (UA)
Gibraltar (GI)	Norway (NO)	United Arab Emirates (AE)

Greece (GR)	Oman (OM)	United Kingdom (GB)
Hong Kong (HK)	Panama (PA)	United States (US)
Hungary (HU)	Peru (PE)	Venezuela (VE)
Iceland (IS)	Philippines (PH)	Vietnam (VN)

Radio Frequency Ranges

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

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

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

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

Table 11: Tx power, data rates, ranges, and decibels by standard

Standard	Maximum Tx power (See Note 1)	Data rate (See Note 2)	Range	Receiver sensitivity
802.11a				
	16 dBm	6 Mbps	604 ft (184 m)	-91 dBm
		9 Mbps	604 ft (184 m)	-90 dBm
		12 Mbps	551 ft (168 m)	-88 dBm
		18 Mbps	545 ft (166 m)	-86 dBm
		24 Mbps	512 ft (156 m)	-82 dBm
		36 Mbps	420 ft (128 m)	-80 dBm
		48 Mbps	322 ft (98 m)	-77 dBm
		54 Mbps	289 ft (88 m)	-75 dBm
802.11g				

Standard	Maximum Tx power (See Note 1)	Data rate (See Note 2)	Range	Receiver sensitivity
	16 dBm	6 Mbps	709 ft (216 m)	-91 dBm
		9 Mbps	650 ft (198 m)	-90 dBm
		12 Mbps	623 ft (190 m)	-87 dBm
		18 Mbps	623 ft (190 m)	-86 dBm
		24 Mbps	623 ft (190 m)	-82 dBm
		36 Mbps	495 ft (151 m)	-80 dBm
		48 Mbps	413 ft (126 m)	-77 dBm
		54 Mbps	394 ft (120 m)	-76 dBm
802.11b				
	17 dBm	1 Mbps	1,010 ft (308 m)	-96 dBm
		2 Mbps	951 ft (290 m)	-85 dBm
		5.5 Mbps	919 ft (280 m)	-90 dBm
		11 Mbps	902 ft (275 m)	-87 dBm

Note

1 Adjusts dynamically when associating with an AP if the AP client setting is enabled.

2 Advertised rates by the APs are used. If the Restricted Data Rates functionality is enabled in the Cisco Unified Communications Manager Administration phone configuration, then the Traffic Stream Rate Set IE (CCX V4) is used.

For more information about supported data rates, Tx power and Rx sensitivity for WLANs, see the *Cisco Unified IP Phone 9971 Wireless LAN Deployment Guide* at this location:

http://www.cisco.com/en/US/products/ps10453/products_implementation_design_guides_list.html

Wireless Modulation Technologies

Wireless communications use the following modulation technologies for signaling:

Direct-Sequence Spread Spectrum (DSSS)

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

Orthogonal Frequency Division Multiplexing (OFDM)

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

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

Table 12: Data Rates, Number of Channels, and Modulation Technologies by IEEE Standard

Item	802.11b	802.11g	802.11a
Data rates	1, 2, 5.5, 11 Mbps	6, 9, 12, 18, 24, 36, 48, 54 Mbps	6, 9, 12, 18, 24, 36, 48, 54 Mbps
Nonoverlapping channels	3 (Japan uses 4)	3	Up to 23
Wireless modulation	DSSS	OFDM	OFDM

AP Channel and Domain Relationships

APs transmit and receive RF signals over channels within the 2.4 GHz or 5 GHz frequency band. To provide a stable wireless environment and reduce channel interference, you must specify nonoverlapping channels for each AP. The recommended channels for 802.11b and 802.11g in North America are 1, 6, and 11.

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

For more information about AP channel and domain relationships, see *Cisco Unified IP Phone 9971 Wireless LAN Deployment Guide* at this location:

http://www.cisco.com/en/US/products/ps10453/products_implementation_design_guides_list.html

Related Topics

VoIP WLAN Deployment, on page 97

WLANs and Roaming

The Cisco Unified IP Phone 9971 supports Cisco Centralized Key Management (CCKM), a centralized key management protocol, and provides a cache of session credentials on the wireless domain server (WDS). APs must register to the WDS for fast roaming to work. CCKM is also supported on the Cisco Unified Wireless LAN Controller alone.

The Cisco Unified IP Phone 9971 supports CCKM with 802.1x+WEP or WPA(TKIP) only. CCKM is not supported with WPA2 or WPA(AES). For details about CCKM, see the Cisco Fast Secure Roaming Application Note at:

http://www.cisco.com/en/US/products/hw/wireless/ps4570/prod_technical_reference09186a00801c5223.html

Related Topics

Voice QoS in Wireless Network, on page 91
VoIP WLAN Deployment, on page 97

Bluetooth Wireless Technology

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

- Use 802.11a that operates in the 5 GHz band.
- Reduce the proximity of other 802.11b/g devices, Bluetooth devices, microwave ovens, and large metal objects.

Related Topics

Bluetooth Wireless Headsets, on page 63

VoIP Wireless Network Components

The Cisco Unified IP Phone must interact with several network components in the WLAN to successfully place and receive calls.

Cisco Unified Wireless AP Interactions

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

Because the Cisco Unified IP Phone 9971 is a desktop (not mobile) phone, changes in the local environment can cause phones to roam between access points and can affect the voice and video performance. In contrast, data users remain in one place or occasionally move to another location. The ability to roam while maintaining

a call is one of the advantages of wireless voice, so RF coverage needs to include stairwells, elevators, quiet corners outside conference rooms, and passageways.

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

After deploying and using wireless voice, you should continue to perform postinstallation site surveys. When you add a group of new users, install more equipment, or stack large amounts of inventory, you are changing the wireless environment. A postinstallation survey verifies that the AP coverage is still adequate for optimal voice communications.

Note Packet loss occurs during roaming; however, the security mode and the presence of fast roaming determines how many packets are lost during transmission.

For more information about Voice QoS in a wireless network, see *Cisco Unified IP Phone 9971 Wireless LAN Deployment Guide* at:

http://www.cisco.com/en/US/products/ps10453/products_implementation_design_guides_list.html

AP Association

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

- Received Signal Strength Indicator (RSSI):Signal strength of available APs within the RF coverage area. The phone attempts to associate with the AP with the highest RSSI value.
- Traffic Specification (TSpec): Calculation of call limits and WLAN load balancing. The TSpec value of each voice stream allows the system to allocate bandwidth to voice devices on a first-come, first-served basis.

The Cisco Unified IP Phone associates with the AP that has the highest RSSI and lowest channel usage values (QBSS) that posses matching SSID and encryption types. To ensure that voice traffic is handled properly, you must configure the correct QoS in the AP.

Related Topics

Voice QoS in Wireless Network, on page 91
Security for Voice Communications in WLANs, on page 93
VoIP WLAN Deployment, on page 97

Voice QoS in Wireless Network

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

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

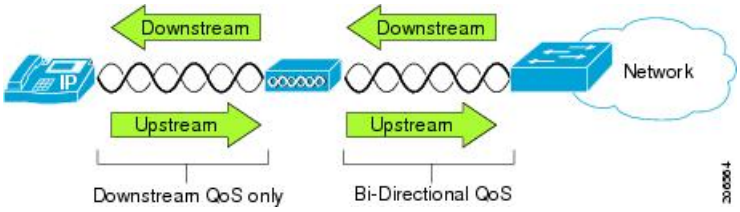
- Voice VLAN: Voice traffic to and from the wireless IP Phone
- Native VLAN: Data traffic to and from other wireless devices

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

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

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

Figure 4: Voice Traffic in a Wireless Network



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

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

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

Note The Cisco Unified IP Phone marks the SCCP signaling packets with a DSCP value of 24 (CS3) and RTP packets with DSCP value of 46 (EF).

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

bandwidth, when the amount of voice traffic is increased beyond this limit (to N+1 calls), the quality of all calls suffers.

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

Implementing QoS in the connected Ethernet switch is highly desirable to maintain good voice quality. The COS and DSCP values that the Cisco Unified IP Phone sets do not need to be modified.

Note The Cisco Unified IP Phone 9971 does not support Video CAC; however, Voice CAC is supported for WLANs.

Related Topics

Authentication Methods, on page 94
Cisco Unified Communications Manager Interaction, on page 93
VoIP WLAN Deployment, on page 97

Cisco Unified Communications Manager Interaction

Cisco Unified Communications Manager is the call control component in the network that handles and routes calls for the wireless IP phones. Cisco Unified Communications Manager manages the components of the IP telephony system (the phones, access gateways, and the resources) for such features as call conferencing and route planning. When you deploy a Cisco Unified IP Phone on a wireless LAN, you must use Cisco Unified Communications Manager Release 7.1(3) or later and the SIP protocol.

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

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

Related Topics

Cisco Unified IP Phone Setup in Cisco Unified Communications Manager, on page 35

Security for Voice Communications in WLANs

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

Authentication Methods

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 Unified IP Phone 9971 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.
- Shared Key Authentication: The AP sends an unencrypted challenge text string to any device that attempts to communicate with the AP. The device that is requesting authentication uses a preconfigured WEP key to encrypt the challenge text and sends it back to the AP. If the challenge text is encrypted correctly, the AP allows the requesting device to authenticate. A device can authenticate only if the device WEP key matches the WEP key on the APs.

  Shared key authentication can be less secure than open authentication with WEP because someone can monitor the challenges. An intruder can calculate the WEP key by comparing the unencrypted and encrypted challenge text strings.
- Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) Authentication: This client server security architecture encrypts EAP transactions within a Transport Level Security (TLS) tunnel between the AP and the RADIUS server, such as the Cisco Access Control Server (ACS).

  The TLS tunnel uses Protected Access Credentials (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 master 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.
- Light Extensible Authentication Protocol (LEAP): Cisco proprietary password-based mutual authentication scheme between the client (phone) and a RADIUS server. Cisco Unified IP Phone can use LEAP for authentication with the wireless network.
- Auto (AKM): Selects the 802.11 Authentication mechanism automatically from the configuration information that the AP, WPA-PSK, or WPA exhibits.

Authenticated Key Management

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

- WPA/WPA2: Uses RADIUS server information to generate unique keys for authentication. Because these keys are generated at the centralized RADIUS server, WPA/WPA2 provides more security than WPA preshared keys that are stored on the AP and phone.
- Cisco Centralized Key Management (CCKM): Uses RADIUS server and a wireless domain server (WDS) information to manage and authenticate keys. The WDS creates a cache of security credentials for CCKM-enabled client devices for fast and secure reauthentication.

With WPA/WPA2 and CCKM, encryption keys are not entered on the 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.

Note Only WPA(TKIP) and 802.1x(WEP) support CCKM.

Encryption Methods

To ensure that voice traffic is secure, the Cisco Unified IP Phone supports WEP, TKIP, and Advanced Encryption Standards (AES) for encryption. When these mechanisms are used for encryption, both the signalling Skinny Client Control Protocol (SCCP) packets and voice Real-Time Transport Protocol (RTP) packets are encrypted between the AP and the Cisco Unified 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 Unified 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 Unified IP Phone supports a key size of 256 bits.

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

AP Authentication and Encryption Options

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

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

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

Note

- When 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.
- When you use Auto (AKM), encryption options are automatically configured for WPA, WPA2, WPA Pre-shared key, WPA2 Pre-shared key, or CCKM.
- In AKM mode, the phone authenticates with LEAP if the phone is configured with WPA, WPA2, or CCKM key management, or if 802.1x is used.
- The Cisco Unified 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 Unified IP Phone supports. The table shows the network configuration option for the phone that corresponds to the AP configuration.

Table 13: Authentication and Encryption Schemes

Cisco AP configuration			**Cisco Unified IP Phone configuration**
Authentication	Key management	Common encryption	Authentication
Open		None	Open
Open (Static WEP)		WEP	Open+WEP
Shared key (Static WEP)		WEP	Shared+WEP
LEAP 802.1x	Optional CCKM	WEP	LEAP or Auto (AKM)

Cisco AP configuration			Cisco Unified IP Phone configuration
LEAP WPA	WPA with optional CCKM	TKIP	LEAP or Auto (AKM)
LEAP WPA2	WPA2	AES	LEAP or Auto (AKM)
EAP-FAST 802.1x	Optional CCKM	WEP	EAP-FAST
EAP-FAST with WPA	WPA Optional CCKM	TKIP	EAP-FAST
EAP-FAST with WPA2	WPA2	AES	EAP-FAST
WPA-PSK	WPA-PSK	TKIP	Auto (AKM)
WPA2-PSK	WAP2-PSK	AES	Auto (AKM)

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

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

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

Related Topics

Cisco Unified Wireless AP Interactions, on page 90
Authentication Methods, on page 94
Encryption Methods, on page 95
Cisco Unified Communications Manager Interaction, on page 93
VoIP Wireless Network Components, on page 90
VoIP WLAN Deployment, on page 97

VoIP WLAN Deployment

This section provides configuration guidelines for deploying Cisco Unified IP Phones in the WLAN.

Supported Access Points

The wireless Cisco Unified IP Phone 9971 is supported on both the Cisco autonomous and unified solutions. Minimum and recommended versions are:

- Cisco IOS Access Points (Autonomous)
  - Minimum = 12.3(8)JEA2 or later
  - Recommended = 12.4(10b)JA3 or later (Does not apply to Cisco Aironet Series 1100, 1140, 1200, or 1230).
- Cisco Unified Wireless LAN Controller
  - Minimum = 5.1.163.0 or later
  - Recommended = 5.2.193.0 or later

Supported APs and Modes

The following table lists the modes that each Cisco Access Point supports.

Table 14: Supported APs and Modes

AP models	802.11b	802.11g	802.11a	Autonomous mode	Unified mode
Cisco Aironet 500 Series	Yes	Yes	No	Yes	Yes
Cisco Aironet 1100 Series	Yes	Yes	No	Yes	Yes
Cisco Aironet 1130 AG Series	Yes	Yes	Yes	Yes	Yes
Cisco Aironet 1140 Series	Yes	Yes	Yes	Yes	Yes
Cisco Aironet 1200 Series	Yes	Yes	Optional	Yes	Yes
Cisco Aironet 1230 AG Series	Yes	Yes	Yes	Yes	Yes
Cisco Aironet 1240 AG Series	Yes	Yes	Yes	Yes	Yes
Cisco Aironet 1250 Series	Yes	Yes	Yes	Yes	Yes
Cisco Aironet 1300 Series	Yes	Yes	No	Yes	Yes

Note The Cisco Unified IP Phone 9971 does not support Voice over the Wireless LAN (VoWLAN) via Outdoor MESH technology (Cisco 1500 series).

No support exists for third-party access points because no interoperability testing occurs with these access points. However, if the access point supports the key features and follows the standards, the Cisco Unified Wireless IP Phone is compliant.

Wi-Fi compliant APs that are manufactured by third-party vendors support the Cisco Unified Wireless IP Phone 9971, but might not support key features such as Wi-Fi MultiMedia (WMM), Unscheduled Auto Power Save Delivery (U-APSD), Traffic Specification (TSPEC), QoS Basic Service Set (QBSS), Dynamic Transmit Power Control (DTPC), or proxy ARP.

Supported Antennas

Some Cisco access points require or allow external antennas. See the following URL for the list of supported antennas and how these external antennas should be mounted:

http://www.cisco.com/en/US/prod/collateral/wireless/ps7183/ps469/product_data_sheet09186a008008883b.html

Note The Cisco Aironet Series 1130 and 1140 access points must be mounted on the ceiling because they possess omnidirectional antennas.

Set Up Wireless LAN

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

If the Wi-Fi connectivity for voice and video is enabled for the Cisco Unified IP Phone 9971, you authenticate the Wi-Fi network by using the WLAN Sign in application within your applications menu.

To enable the application, go to **Applications** > **Administrator Settings** > **Network Setup** > **Wireless Setup** > **WLAN Sign in Access** and enable WLAN network.

To change the username or password, go to **Applications** > **Administrator Settings**.

For complete configuration information, see the *Cisco Unified IP Phone 9971 Wireless LAN Deployment Guide* at this location:

http://www.cisco.com/en/US/products/ps10453/products_implementation_design_guides_list.html

The *Cisco Unified IP Phone 9971 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 Unified IP Phone 9971

Set Up Wireless LAN in Cisco Unified Communications Manager Administration

In Cisco Unified Communications Manager Administration, you must enable a parameter called “Wi-Fi” for the wireless Cisco Unified IP Phone 9971. This can be done in one of the following locations in Cisco Unified Communications Manager Administration:

- To enable wireless LAN on a specific phone, select the enable setting for the Wi-Fi parameter in the Product Specific Configuration Layout section (**Device** > **Phone**) for the specific phone, and check the Override Common Settings check box.

- To enable wireless LAN for a group of phones, select the enable setting for the Wi-Fi parameter in a Common Phone Profile Configuration window (**Device** > **Device Settings** > **Common Phone Profile**), check the Override Common Settings check box, then associate the phone (**Device** > **Phone**) with that common phone profile.
- To enable wireless LAN for all WLAN-capable phones in your network, select the enable setting for the Wi-Fi parameter in the Enterprise Phone Configuration window (**System** > **Enterprise Phone Configuration**), and check the Override Common Settings check box.

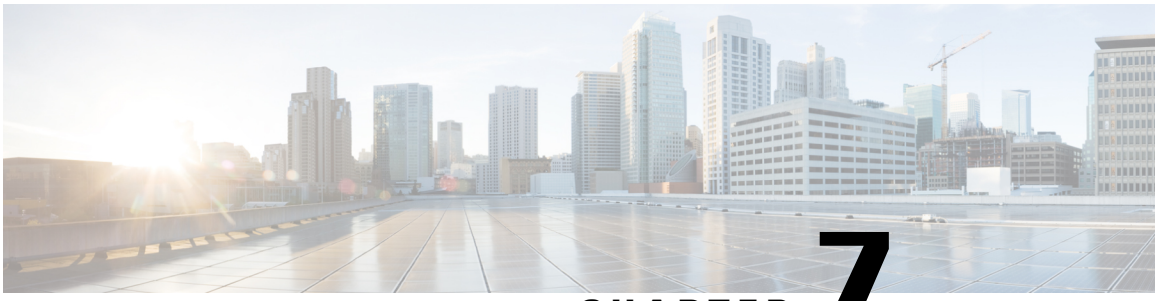
Note In the Phone Configuration window in Cisco Unified Communications Manager Administration (**Device** > **Phone**), use the wired-line MAC address when you configure the MAC address. Cisco Unified Communications Manager registration does not use the wireless MAC address.

Wireless LAN on Cisco Unified IP Phone setup

Before the 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 Wireless Setup submenu and set up the WLAN configuration.

Related Topics

Wireless Setup menu, on page 108



CHAPTER 7

Cisco Unified IP Phone Settings

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

This chapter includes the following topics:

Cisco Unified IP Phone Setup Menus

The Cisco Unified IP Phone includes the following configuration menus:

- Network Setup: Provides options for viewing and configuring network settings such as IPv4, IPv6, WLAN, and Ethernet.
  - Ethernet Setup: The menu items in this submenu provide configuration options to configure the Cisco Unified IP Phone over an ethernet network.
  - Wireless Setup: The menu items in this submenu provide configuration options to configure the Cisco Unified IP Phone with the wireless local area network (WLAN).

Note The Wireless Setup menu only displays on the Cisco Unified IP Phone 9971 when Wi-Fi is enabled on the Cisco Unified Communications Manager.

  - IPv4 Setup and IPv6 Setup: These submenus of the Ethernet Setup menu and of the Wireless Setup menu provide additional network options.

- Security Setup: Provides options for viewing and configuring security settings such as security mode, the trust list and 802.1X authentication.

Before you can change option settings on the Network Setup menu, you must unlock options for editing.

You can control whether a phone user has access to phone settings by using the Settings Access field in the Product Specific portion of the Phone Configuration window in Cisco Unified Communications Manager Administration.

Related Topics

IPv6 Setup menu fields, on page 120
Ethernet Setup menu, on page 104
Wireless Setup menu, on page 108
IPv4 Setup Menu Options, on page 113
Security Setup Menu, on page 123

Display Setup Menu

To display a configuration menu, follow these steps:

Procedure

Step 1 Press **Applications** .

Step 2 Select **Administrator Settings**.

Step 3 Select **Network Setup** or **Security Setup**.

Note For information about the Status menu, see Model information, status, and statistics, on page 225. For information about the Reset Settings menu, see Troubleshooting and Maintenance, on page 267.

Step 4 Enter your user ID and password, if required, then click **Sign-In**.

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 **Exit** or the back arrow .

Related Topics

Password Protection, on page 103
Value Input Guidelines, on page 103
Ethernet Setup menu, on page 104
Wireless Setup menu, on page 108
IPv4 Setup Menu Options, on page 113
Security Setup Menu, on page 123

Password Protection

You can apply a password to the phone so that no changes can be made to the administrative options on the phone without password entry on the Administrator Settings phone screen.

Apply Phone Password

To apply a password to the phone, perform these steps:

Procedure

Step 1 In Cisco Unified Communications Manager Administration, navigate to the Common Phone Profile Configuration window using **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.

Value Input Guidelines

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, then press **Select** in the navigation pad to activate that field. You can also double-tap on an editable field to activate it for editing. 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 arrow softkey if you make a mistake. This softkey deletes the character to the left of the cursor.
- Press **Cancel** before pressing **Save** to discard any changes that you made.
- To enter an IP address, you enter values into four segments already divided for you. When you have finished entering the leftmost digits before the first period, use the right arrow key to move to the next segment. The period that follows the leftmost digits is automatically inserted.
- To enter the colon in an IPv6 address, press the asterisk (*) on the keypad.

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

Related Topics

Display Setup Menu, on page 102
Password Protection, on page 103
Ethernet Setup menu, on page 104
Wireless Setup menu, on page 108
IPv4 Setup Menu Options, on page 113
Basic Reset, on page 290

Ethernet Setup menu

The Ethernet Setup menu provides options for viewing and changing a variety of network settings. The following table describes these options and, where applicable, explains how to change them.

Note Establishing a VPN connection overwrites the Ethernet data fields.

Table 15: Ethernet Setup menu options

Option	Description	To change
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 IPv4 Setup Menu Options, on page 113.	Scroll to IPv4 Setup and press **Select**.
IPv6 Setup	IPv6 address of the phone. This option display only when the phone is configured in IPv6-only mode or in dual-stack mode. For more information about the IPv4 address fields, see IPv6 Setup menu fields, on page 120.	Scroll to IPv6 Setup and press **Select**.
MAC Address	Unique Media Access Control (MAC) address of the phone.	Display only. Cannot configure.

Option	Description	To change
Domain Name	Name of the Domain Name System (DNS) domain in which the phone resides.	See Set Domain Name Field, on page 107.
Operational VLAN ID	Auxiliary Virtual Local Area Network (VLAN) configured on a Cisco Catalyst switch of which the phone is a member. If the phone has not received an auxiliary VLAN, this option indicates the Administrative VLAN. If neither the auxiliary VLAN nor the Administrative VLAN are configured, this option is blank.	Display only. Cannot configure. The phone obtains the Operational VLAN ID via Cisco Discovery Protocol (CDP) or Link Level Discovery Protocol Media Endpoint Discovery (LLDP-MED). This information comes from the switch to which the phone is attached. To assign a VLAN ID manually, use the Admin VLAN ID option.
Admin. VLAN ID	Auxiliary VLAN of which the phone is a member. Used only if the phone does not receive an auxiliary VLAN from the switch; otherwise, this value is ignored.	See Set Admin VLAN ID Field, on page 107.
PC VLAN	Allows the phone to interoperate with third-party switches that do not support a voice VLAN. The Admin VLAN ID option must be set before you can change this option.	See Set PC VLAN Field, on page 107.

Option	Description	To change
SW Port Setup	Speed and duplex of the network port. Valid values specify: • Auto Negotiate • 1000 Full:1000-BaseT/full duplex • 100 Half: 100-BaseT/half duplex • 100 Full: 100-BaseT/full duplex • 10 Half: 10-BaseT/half duplex • 10 Full: 10-BaseT/full duplex If the phone is connected to a switch, configure the port on the switch to the same speed/duplex as the phone, or configure both to autonegotiate. If you change the setting of this option, you must change the PC Port Configuration option to the same setting.	See Set SW Port Configuration Field, on page 108.
PC Port Setup	Speed and duplex of the Computer (access) port. Valid values: • Auto Negotiate • 1000 Full: 1000-BaseT/full duplex • 100 Half: 100-BaseT/half duplex • 100 Full: 100-BaseT/full duplex • 10 Half: 10-BaseT/half duplex • 10 Full: 10-BaseT/full duplex If the phone is connected to a switch, configure the port on the switch to the same speed/duplex as the phone, or configure both to autonegotiate. If you change the setting of this option, you must change the SW Port Configuration option to the same setting.	See Set PC Port Configuration Field, on page 108. To configure the setting on multiple phones simultaneously, enable Remote Port Configuration in the Enterprise Phone Configuration window(**System** > **Enterprise Phone Configuration**). **Note** If the ports are configured for Remote Port Configuration in Cisco Unified Communications Manager Administration, the data cannot be changed on the phone.

Related Topics

Display Setup Menu, on page 102
Password Protection, on page 103
Value Input Guidelines, on page 103
Wireless Setup menu, on page 108
IPv4 Setup Menu Options, on page 113

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**.

Set Admin VLAN ID Field

Procedure

Step 1 Scroll to the Admin. VLAN ID option, press **Select**, and enter a new Admin VLAN setting.
Step 2 Press **Apply**.

Set PC VLAN Field

Procedure

Step 1 Ensure that the Admin VLAN ID option is set.
Step 2 Scroll to the PC VLAN option, press **Select**, and then enter a new PC VLAN setting.
Step 3 Press **Apply**.

Set SW Port Configuration Field

Procedure

Step 1 Unlock network configuration options.
Step 2 Scroll to the SW Port Configuration option and press **Select**.
Step 3 Scroll to the setting that you want and press **Select**.

Set PC Port Configuration Field

Procedure

Step 1 Unlock network configuration options.
Step 2 Scroll to the PC Port Configuration option and press **Select**.
Step 3 Scroll to the setting that you want and press **Select**.

Wireless Setup menu

The Wireless Setup menu provides options on the Cisco Unified IP Phone 9971 to view and make a variety of network settings. The following table describes these options and, where applicable, explains how to change them.

Note You can configure the Wireless settings only on the Cisco Unified IP Phone keypad. You must use the AC adapter when you use the Cisco Unified IP Phone in Wireless mode. Wireless is disabled when Ethernet is connected.

Note The Wireless Setup option does not appear in the Network Setup menu when WiFi is disabled on the Cisco Unified Communications Manager.

Table 16: WirelessSetup menu options

Option	Description	To change
Wireless	Turns the wireless radio on Cisco Unified IP Phone on or off. Valid values specify: • On: Turns the wireless radio on the phone on. • Off: Turns the wireless radio on the phone off. Default: On	See Set Wireless Field, on page 111.
Wireless Sign in Access	Enables the display of the Wireless Sign in Access window in the main Applications menu: • On: The Wireless Sign In Access window displays. Turning this value on allows you to sign in or change your Wireless user ID and password on the main Applications menu. Otherwise, to change your sign-in information, navigate down to the Security menu level and select either the LEAP or EAP-FAST methods, both of which require sign-in credentials. • Off: The Wireless Sign In Access window does not display. Default: Off	See Set Wireless Sign in Access Field, on page 111.
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 IPv4 Setup Menu Options, on page 113.	Scroll to IPv4 Setup and press **Select**.
MAC Address	Unique Media Access Control (MAC) address of the phone.	Display only. Cannot configure.

Option	Description	To change
Domain Name	Name of the Domain Name System (DNS) domain in which the phone resides.	See Set Domain Name Field, on page 112.
SSID	Specifies the Service Set Identifier, a unique identifier for accessing wireless access points.	See Set SSID Field, on page 112.
Security Mode	The type of authentication that the phone uses to access the WLAN. Valid values specify: • Open: Access to all access points (APs) without encryption. • Open with WEP: Open 802.11 authentication but uses Wired Equivalent Privacy (WEP) for encrypting the data. Specifies access to all APs and authentication through WEP keys at the local AP. • Shared Key: Shared key authentication using WEP. • LEAP: Lightweight Extensible Authentication Protocol authentication exchanges a username and cryptographically secure password with a RADIUS server in the network. LEAP is a Cisco proprietary version of EAP. LEAP supports WPA and WPA2. • EAP-FAST: Extensible Authentication Protocol Flexible Authentication via Secure Tunneling exchanges a username and cryptographically secure password with a RADIUS server in the network where a PAC (Protected Access Credential) establishes a secure tunnel for authentication. EAP-FAST supports WPA and WPA2. • AKM: Selects the 802.11 authentication mechanism automatically from the configuration information that the access point exhibits. WPA-PSK or WPA versions 1 or 2 can be used if they are configured for this mode.	See Set Security Mode Field, on page 112.

Option	Description	To change
802.11 Mode	Specifies the wireless signal standard that is used in the WLAN. Valid values specify: • Auto: Default value. Gives precedence to 5.0 Ghz if available. • 802.11a • 802.11b/g	See Set 802.11 Mode Field, on page 112.

Notes

Consider the following when you select AKM:

1 AKM uses LEAP for 802.1x when WPA, WPA2, or CCKM is in use.

2 AKM selects the encryption method by giving precedence to the strongest key management type and then the strongest cipher.

3 CCKM is not supported with WPA2.

Related Topics

Display Setup Menu, on page 102
Value Input Guidelines, on page 103

Set Wireless Field

Procedure

Step 1 Scroll to the Wireless option, and use the toggle switch to change the setting between on and off.

Step 2 Press **Apply**.

Set Wireless Sign in Access Field

Procedure

Step 1 Scroll to the Wireless Sign In option, and use the toggle switch to change the setting between on and off.

Step 2 Press **Apply**.

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**.

Set SSID Field

Procedure

Step 1 Scroll to the SSID option, press **Select**, and enter an SSID.
Step 2 Press **Apply**.

Set Security Mode Field

Procedure

Step 1 Scroll to the Security Mode option, and highlight the desired value.
Step 2 Click **Apply**.

Set 802.11 Mode Field

Procedure

Step 1 Scroll to the 802.11 Mode option, and highlight the desired value.
Step 2 Click **Apply**.

IPv4 Setup Menu Options

The IPv4 Setup menu is a submenu of the Ethernet Setup menu and of the Wireless Setup menu. To reach the IPv4 menu, select the IPv4 option on the Ethernet Setup menu or on the Wireless Setup menu.

The following table describes the IPv4 Setup menu options.

Table 17: IPv4 Setup Menu Options

Option	Description	To change
DHCP Enabled	Indicates whether the phone has DHCP enabled or disabled. When DHCP is enabled, the DHCP server assigns the phone an IP address. When DHCP is disabled, the administrator must manually assign an IP address to the phone. For more information, see DHCP Usage, on page 118.	See Set DHCP Enabled Field, on page 116.
IP Address	Internet Protocol (IP) address of the phone. If you assign an IP address with this option, you must also assign a subnet mask and default router. See the Subnet Mask and Default Router options in this table.	See Set IP Address Field, on page 116.
Subnet Mask	Subnet mask used by the phone.	See Set Subnet Mask Field, on page 116.
Default Router	Default router used by the phone.	See Set Default Router Field, on page 116.
DNS Server 1 DNS Server 2 DNS Server 3	Primary Domain Name System (DNS) server (DNS Server 1) and optional backup DNS servers (DNS Server 2 and 3) that the phone uses.	See Set DNS Server Fields, on page 117.
Alternate TFTP	Indicates whether the phone is using an alternate TFTP server.	See Set Alternate TFTP Field, on page 117.

Option	Description	To change
TFTP Server 1	Primary Trivial File Transfer Protocol (TFTP) server that the phone uses. If you are not using DHCP in your network and you want to change this server, you must use the TFTP Server 1 option. If you set the Alternate TFTP option to yes, 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. 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 IPv6 TFTP servers **2** Any manually assigned IPv4 TFTP servers **3** DHCPv6 assigned TFTP servers **4** DHCP assigned TFTP servers **Note** For information about the CTL and ITL files, see the *Cisco Unified Communications Manager Security Guide*.	See Set TFTP Server 1 Field, on page 117.

Option	Description	To change
TFTP Server 2	Optional backup TFTP server that the phone uses if the primary TFTP server is unavailable. 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 either of the files before you can save changes to the TFTP Server 2 option. In this case, the phone deletes either of the files when you save changes to the TFTP Server 2 option. A new CTL or ITL file downloads from the new TFTP Server 2 address. When the phone looks for the TFTP server, it 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 the following order: **1** Manually assigned IPv6 TFTP servers **2** Manually assigned IPv4 TFTP servers **3** DHCPv6 assigned TFTP servers **4** DHCP assigned TFTP servers **Note** For information about the CTL or ITL file, see Cisco Unified Communications Manager Security Guide.	See Set TFTP Server 2 Field, on page 118. If you forget to unlock the CTL or ITL file, you can change the TFTP Server 2 address in either file, then erase them by pressing Erase from the Security Configuration menu. A new CTL or ITL file downloads from the new TFTP Server 2 address.
BOOTP Server	Indicates whether the phone received the IP address from a BOOTP server rather than from a DHCP server.	Display only.
DHCP Address Released	Releases the IP address that DHCP assigned.	This field is editable if DHCP is enabled. If you wish to remove the phone from the VLAN and release the IP address for reassignment, set this option to Yes and press Apply.

Related Topics

Display Setup Menu, on page 102
Password Protection, on page 103
Value Input Guidelines, on page 103

Set DHCP Enabled Field

Procedure

Step 1 Scroll to the DHCP Enabled option.
Step 2 Press **No** to disable DHCP, or press **Yes** to enable DHCP.

Set IP Address Field

Procedure

Step 1 Set the DHCP Enabled option to **No**.
Step 2 Scroll to the IP Address option, press **Select**, and enter a new IP Address.
Step 3 Press **Apply**.

Set Subnet Mask Field

Procedure

Step 1 Set the DHCP Enabled option to **No**.
Step 2 Scroll to the Subnet Mask option, press **Select**, and enter a new subnet mask.
Step 3 Press **Apply**.

Set Default Router Field

Procedure

Step 1 Set the DHCP Enabled option to **No**.
Step 2 Scroll to the appropriate Default Router option, press **Select**, and enter a new router IP address.
Step 3 Press **Apply**.

Set DNS Server Fields

Procedure

Step 1 Set the DHCP Enabled option to **No**.
Step 2 Scroll to the appropriate DNS Server option, press **Select**, and enter a new DNS server IP address.
Step 3 Press **Apply**.
Step 4 Repeat Steps 2 and 3 as needed to assign backup DNS servers.

Set Alternate TFTP Field

Procedure

Step 1 Scroll to the Alternate TFTP option.
Step 2 Press **Yes** if the phone should use an alternative TFTP server.
Step 3 Press **No** if the phone should not use an alternative TFTP server.

Set TFTP Server 1 Field

Procedure

Step 1 Unlock the CTL or ITL file if necessary (for example, if you are changing the administrative domain of the phone). If the CTL and ITL files both exist, unlock either file.
Step 2 If DHCP is enabled, set the Alternate TFTP option to **Yes**.
Step 3 Scroll to the TFTP Server 1 option, press **Select**, and enter a new TFTP server IP address.
Step 4 Press **Apply** then press **Save**.

Set TFTP Server 2 Field

Procedure

Step 1 Unlock the CTL or ITL file if necessary (for example, if you are changing the administrative domain of the phone). If both the CTL and ITL files exist, unlock either of the files.

Step 2 Unlock network configuration options.

Step 3 Enter an IP address for the TFTP Server 1 option.

Step 4 Scroll to the TFTP Server 2 option, press **Select**, and enter a new backup TFTP server IP address. If there is no secondary TFTP Server, you can use **Delete** to clear the field of a previous value.

Step 5 Press **Apply** and then press **Save**.

DHCP Usage

If you are configuring the Ethernet network settings on the phone for an IP network, you can set up an IP address for the phone by either using DHCP or manually entering an IP address.

Note You must also enter the domain name for the phone in the Ethernet Setup page.

Set Up Phone To Use DHCP

To enable DHCP and allow the DHCP server to automatically assign an IP address to the Cisco Unified IP Phone and direct the phone to a TFTP server, perform these steps:

Procedure

Step 1 Press **Applications** and choose **Administrator Settings** > **Network Setup** > **Ethernet Setup** > **IPv4 Setup**.

Step 2 To enable DHCP, set DHCP Enabled to **Yes**. DHCP is enabled by default.

Step 3 To use an alternate TFTP server, set Alternate TFTP Server to **Yes**, and enter the IP address for the TFTP Server.

Note Consult with the network administrator to determine whether you need to assign an alternative TFTP server instead of using the TFTP server that DHCP assigns.

Step 4 Press **Apply**,

Set Up Phone To Not Use DHCP

When not using DHCP, you must configure the IP address, subnet mask, TFTP server, and default router locally on the phone.

Procedure

Step 1 Press **Applications** and choose **Administrator Settings** > **Network Setup** > **Ethernet Setup** > **IPv4 Setup**.

Step 2 To disable DHCP and manually set an IP address:

a) Set DHCP Enabled to **No**.
b) Enter the static IP address for phone.
c) Enter the subnet mask.
d) Enter the default router IP addresses.
e) Set Alternate TFTP Server to **Yes**, and enter the IP address for TFTP Server 1.

Step 3 Press **Apply**.

IPv6

IPv6 addressing is supported on the phone. A valid IPv6 address is 128 bits in length, including the subnet prefix.

IPv6 addresses must be in one of the following formats:

- Eight sets of four hexadecimal digits separated by colons where the leftmost digits represent the highest-order bits. Any leading or trailing zeros in each group may be omitted.
- Compressed format to collapse a single run of consecutive zero groups into a single group represented by a double colon. Note that this can only be done once in an address.

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 (dual-stack). 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 to Unified CM.

For more information, see the section on Common Device Configuration in *Cisco Unified Communications Manager Feature and Services Guide*, “IPv6 Support in Cisco Unified Communications Devices”.

Note Cisco recommends IPv4 and IPv6 as the setting for the phone addressing mode. IPv6 Only is not recommended for production environments.

IPv6 Setup menu fields

The IPv6 Setup menu is a submenu of Network settings and is accessed from the Administrator Settings menu.

- For Cisco Unified IP Phones 8961 and 9951: navigate to the IPv6 options from **Administrator Settings** > **Ethernet Setup** > **IPv6 Setup**.
- For Cisco Unified IP Phone 9971 with Wi-Fi disabled on the Cisco Unified Communications Manager: navigate to the IPv6 options from **Administrator Settings** > **Ethernet Setup** > **IPv6 Setup**.
- For Cisco Unified IP Phone 9971 with Wi-Fi enabled on the Cisco Unified Communications Manager: navigate to **Administrator Settings** > **Network Setup** > **Wireless Setup** > **IPv6 Setup**.

The following table describes the IPv6 related information found in the IPv6 menu.

Table 18: IPv6 Setup menu options

Option	Default value	Description
DHCPv6 Enabled	Yes	Allows the user to enable or disable DHCPv6. When DHCPv6 is enabled, the DHCPv6 server assigns the phone an IPv6 address. When DHCPv6 is disabled, the administrator must assign the IPv6 address. **Note** Unlike DHCPv4, even DHCPv6 is disabled the phone can still generate a Stateless address autoconfiguration (SLAAC) address if autoconfigure is enabled.
IPv6 Address	::	Displays the current IPv6 address of the phone or allows the user to enter a new IPv6 address. Two address formats are supported: • Eight sets of hexadecimal digits separated by colons X:X:X:X:X:X:X:X • Compressed format to collapse a single run of consecutive zero groups into a single group represented by a double colon. If the IP address is assigned with this option, you must also assign the IPv6 prefix length and the default router.
IPv6 Prefix Length	0	Displays the current prefix length for the subnet or allows the user to enter a new prefix length. The subnet prefix length is a decimal value from 1-128.

Option	Default value	Description
IPv6 Default Router	::	Displays the default router used by the phone or allows the user to enter a new IPv6 default router.
IPv6 DNS Server 1	::	Displays the primary DNSv6 server used by the phone or allows the user to enter a new server.
IPv6 DNS Server 2	::	Displays the secondary DNSv6 server used by the phone or allows the user to set a new secondary DNSv6 server.
IPv6 Alternate TFTP	No	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 primary TFTP server.
IPv6 TFTP Server 2	::	(Optional) Displays the secondary IPv6 TFTP server used if the primary IPv6 TFTP server is unavailable or allows the user to set a new secondary TFTP server.
IPv6 Address Released	No	Allows the user to release IPv6-related information.

Edit IPv6 Setup options

This procedure applies to the following phones:

- Cisco Unified IP Phone 8961
- Cisco Unified IP Phone 9951
- Cisco Unified IP Phone 9971 with Wi-Fi disabled on the Cisco Unified Communications Manager

Note If DHCPv6 Enabled is set to Yes, some IPv6 Setup menu options cannot be edited. If you need to change a setting and it is not available, check the value of the DHCPv6 Enabled option.

Procedure

Step 1 Press **Applications**.

Step 2 Select **Administrator Settings** > **Ethernet Setup** > **IPv6 Setup**.

Step 3 Select the option to edit or to toggle.

Step 4 To enter IPv6 addresses,

a) Click in an input field.

b) Make your changes to the field (see the information below).

The following table describes the address formats.

Format	Description
X:X:X:X:X:X:X:X	Eight sets of hexadecimal digits separated by colons. Leading or trailing zeros in each group may be omitted. Example: 2001:db8:0:0:0:52:0:1
Compressed	Collapse a single run of consecutive zero groups into a single group represented by a double colon. Example: 2001:db8::52:0:1

- To enter a colon (:) in the address, press the asterisk (*) on the keypad.
- To enter hexadecimal digits a, b, and c, press 2 on the keypad, scroll to select the required digit, and press **Enter**.
- To enter hexadecimal digits d, e, and f, press 3 on the keypad, scroll to select the required digit, and press **Enter**.
- After you enter each part of the address, you press **Apply** or **Revert** .

Step 5 Change toggle fields using these steps:

a) If an option is set to No, press **Yes** to enable it. If the option is set to Yes, press **No** to disable it.

b) Press **Apply** to save your change, or **Revert** to discard it.

Step 6 Press **Apply** to save your change or press **Revert** to discard the change.

Edit Wireless IPv6 Setup options

This procedure only applies to the Cisco Unified IP Phone 9971 when Wi-Fi is enabled on the Cisco Unified Communications Manager.

Note If DHCPv6 Enabled is set to Yes, some IPv6 Setup menu options cannot be edited. If you need to change a setting and it is not available, check the value of the DHCPv6 Enabled option.

Procedure

Step 1 Press **Applications**.

Step 2 Select **Administrator Settings** > **Network Setup** > **Wireless Setup** > **WLAN IPv6 Setup**.

Step 3 Select the option to edit or to toggle.

Step 4 To enter IPv6 addresses,

a) Click in an input field.

b) Make your changes to the field (see the information below).

The following table describes the address formats.

Format	Description
X:X:X:X:X:X:X:X	Eight sets of hexadecimal digits separated by colons. Leading or trailing zeros in each group may be omitted. Example: 2001:db8:0:0:0:52:0:1
Compressed	Collapse a single run of consecutive zero groups into a single group represented by a double colon. Example: 2001:db8::52:0:1

- To enter a colon (:) in the address, press the asterisk (*) on the keypad.
- To enter hexadecimal digits a, b, and c, press 2 on the keypad, scroll to select the required digit, and press **Enter**.
- To enter hexadecimal digits d, e, and f, press 3 on the keypad, scroll to select the required digit, and press **Enter**.
- After you enter each part of the address, you press **Apply** or **Revert** .

Step 5 Change toggle fields using these steps:

a) If an option is set to No, press **Yes** to enable it. If the option is set to Yes, press **No** to disable it.
b) Press **Apply** to save your change, or **Revert** to discard it.

Step 6 Press **Apply** to save your change or press **Revert** to discard the change.

Security Setup Menu

The Security Setup menu that you access directly from the Administrator Settings menu provides information about various security settings. The menu also provides access to the Trust List menu and indicates whether the CTL or ITL file is installed on the phone.

The following table describes the options in the Security Setup menu.

Table 19: Security Setup Menu

Option	Description	To change
Security Mode	Displays the security mode that is set for the phone.	From Cisco Unified Communications Manager Administration, choose **Device** > **Phone**. The setting appears in the Protocol Specific Information portion of the Phone Configuration window.

Option	Description	To change
LSC	Indicates whether a locally significant certificate that is used for security features is installed on the phone (Yes) or is not installed on the phone (No).	For information about how to manage the LSC for your phone, see the "Using the Certificate Authority Proxy Function" chapter in the *Cisco Unified Communications Manager Security Guide*.
Trust List	The Trust List provides submenus for the CTL, ITL, and Signed Configuration files. The CTL File submenu displays the contents of the CTL file. The ITL File submenu displays contents of the ITL file.	For more information, see Trust List Menu, on page 124.
802.1X Authentication	Allows you to enable 802.1X authentication for this phone.	See 802.1X Authentication and Transaction Status, on page 125.

Related Topics

Display Setup Menu, on page 102

Trust List Menu

The Trust List menu provides a top-level menu that contains CTL, ITL, and the Signed Configuration submenus. The content of the Signed Configuration file is Survivable Remote Site Telephony (SRST).

The Trust List menu only displays components that have associated certificates. The following table describes Trust List menu options.

Table 20: Trust List Menu Settings

Option	Description	To change
CTL Signature	MD5 hash of the CTL file.	For more information about these settings, see the "Configuring the Cisco CTL Client" section in the *Cisco Unified Communications Manager Security Guide*.
Unified CM/TFTP Server	Common name of a Cisco Unified Communications Manager and TFTP server that the phone uses. Also displays a certificate icon if a certificate is installed for this server.	For more information about these settings, see the "Configuring the Cisco CTL Client" section in the *Cisco Unified Communications Manager Security Guide*.

Option	Description	To change
CAPF Server	Common name of the CAPF that the phone uses. Also displays a certificate icon if a certificate is installed for this server.	For more information about these settings, see the "Configuring the Cisco CTL Client" section in the *Cisco Unified Communications Manager Security Guide*.
SRST Router	IP address of the trusted SRST router that is available to the phone, if such a device is configured in Cisco Unified Communications Manager Administration. Also displays a certificate icon if a certificate is installed for this server.	For more information about these settings, see the "Configuring the Cisco CTL Client" section in the *Cisco Unified Communications Manager Security Guide*.

802.1X Authentication and Transaction Status

The 802.1X Authentication Settings menu allows you to enable 802.1X authentication and view transaction status.

Access 802.1X Authentication

You can access the 802.1X authentication settings by following these steps:

Procedure

Step 1 Press **Applications** .

Step 2 Choose **Administrator Settings** > **Security Setup** > **802.1X Authentication**.

Step 3 Configure the options as described in 802.1X Authentication Options, on page 125.

Step 4 To exit this menu, press **Exit**.

802.1X Authentication Options

The following table describes the 802.1X authentication options.

Table 21: 802.1X Authentication Settings

Option	Description	To change
Device Authentication	Determines whether 802.1X authentication is enabled: • Enabled: Phone uses 802.1X authentication to request network access. • Disabled: Default setting. The phone uses CDP to acquire VLAN and network access.	See Set Device Authentication Field, on page 127.
EAP-MD5	Specifies a password for use with 802.1X authentication. The menu options are described in the rows that follow:: • Device ID • Shared Secret • Realm	See Set EAP-MD5 Fields, on page 127.
	Device ID: Derivative of the phone model number and unique MAC address. Displays in this format: CP-<model>-SEP-<MAC>	Display only. Cannot configure.
	Shared Secret: Choose a password to use on the phone and on the authentication server. The password must be between 6 and 32 characters in length and can consist of any combination of numbers or letters. **Note** If you disable 802.1X authentication or perform a factory reset (reset all settings) of the phone, the shared secret is deleted.	See Set EAP-MD5 Fields, on page 127. See Cisco Unified IP Phone Security Problems, on page 273 for assistance in recovering from a deleted shared secret.
	Realm: Indicates the user network domain, always set as Network.	Display only. Cannot configure.

Option	Description	To change
Transaction Status	State: Displays the state of 802.1x authentication: • Disconnected: Indicates that 802.1x authentication is not configured on the phone. • Authenticated: Indicates that the phone is authenticated. • Held: Indicates that the authentication process is in progress. Protocol: Displays the EAP method that is used for 802.1x authentication (can be EAP-MD5, EAP-FAST or EAP-TLS).	Display only. Cannot configure.

Set Device Authentication Field

Procedure

Step 1 After pressing **Applications**  , choose **Administrator Settings** > **Security Setup** > **802.1X Authentication**.

Step 2 Set the Device Authentication option to **Enabled** or **Disabled**.

Step 3 Press **Apply**.

Set EAP-MD5 Fields

Procedure

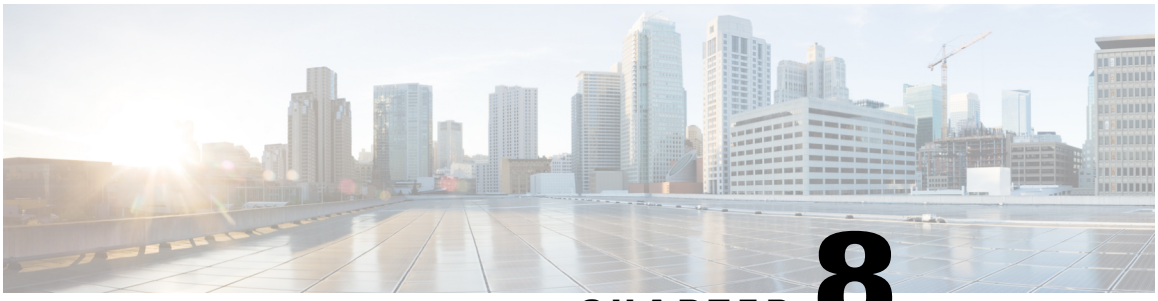
Step 1 Press **Applications**  .

Step 2 Choose **Administrator Settings** > **Security Setup** > **802.1X Authentication** > **EAP-MD5**.

Step 3 To change the shared secret, choose Shared Secret.

Step 4 Enter the shared secret.

Step 5 Press **Apply**.



CHAPTER 8

Features, Templates, Services, and User Setup

After you install Cisco Unified IP Phones in your network, configure their network settings, and add them to Cisco Unified Communications Manager, you must use the Cisco Unified Communications Manager Administration application to configure telephony features, optionally modify phone templates, set up services, and assign users.

This chapter provides an overview of these configuration and setup procedures. Cisco Unified Communications Manager documentation provides detailed instructions for these procedures.

For suggestions about how to provide users with information about features, and what information to provide, see Internal Support Website, on page 295.

For information about setting up phones in non-English environments, see International User Support, on page 301.

This chapter includes following topics:

Telephony features available for Cisco Unified IP Phone

After you add Cisco Unified IP Phones to Cisco Unified Communications Manager, you can add functionality to the phones. The following table includes a list of supported telephony features, many of which you can configure by using Cisco Unified Communications Manager Administration. The Configuration Reference column lists Cisco Unified Communications Manager and other documentation that contains configuration procedures and related information.

For information about using most of these features on the phone, see *Cisco Unified IP Phone 8961, 9951, and 9971 User Guide for Cisco Unified Communications Manager*. Also, see Feature Buttons and Softkeys, on page 171 for a list of features that can be configured as programmable buttons; Feature Buttons and Softkeys, on page 171 also lists whether a feature is a softkey or a dedicated feature button.

Note Cisco Unified Communications Manager Administration also provides several service parameters that you can use to configure various telephony functions. For more information about accessing and configuring service parameters, see *Cisco Unified Communications Manager Administration Guide*. For more information about the functions of a service, click on the name of the parameter or the question mark help button in the Service Parameter Configuration window.

Table 22: Telephony features for the Cisco Unified IP Phone

Feature	Description	Configuration Reference
Actionable Incoming Call Alert	Controls whether the incoming call alert displays as a traditional pop-up alert or as an actionable alert. By default, the Actionable Incoming Call Alert feature is disabled. **Note** If the Custom Line Filters feature is enabled, the Actionable Call Alert Feature applies only to the lines covered by the filters.	For more information, see Actionable Incoming Call Alert Configuration, on page 197.

Feature	Description	Configuration Reference
Agent Greeting	Allows an agent to create and update a prerecorded greeting that plays at the beginning of a call, such as a customer call, before the agent begins the conversation with the caller. The agent can prerecord a single greeting or multiple ones as needed and create and update them. When a customer calls, both callers hear the prerecorded greeting. The agent can remain on mute until the greeting ends or answer the call over the greeting. All codecs supported for the phone are supported for Agent Greeting calls. To enable Agent Greeting in the Cisco Unified Communications Manager Administration application, choose **Device** > **Phone**, locate the IP phone that you want to configure. Scroll to the Device Information Layout pane and set Built In Bridge to On or Default. If Built In Bridge is set to Default, in the Cisco Unified Communications Manager Administration application, choose **System** > **Service Parameters** and select the appropriate Server and Service. Scroll to the Clusterwide Parameters (Device - Phone) pane and set Builtin Bridge Enable to On.	For more information, see: • *Cisco Unified Communications Manager Features and Services Guide*, "Barge and Privacy" chapter • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones" chapter
Alert Calls	An Alert Call is a specific phone number that users considers important and want to be alerted when they receive a call from or dial a call to this number. The Alert Calls feature allows users to view a list of all Alert Calls in chronological order (oldest to most recent) that are received on all of their phone lines. Users interact with this feature using a programmable line key, which makes it easier to view all of the Alert Calls that are received across their phone lines. The Phone Button Template controls the display of the Alert Calls button.	For more information, see *Cisco Unified Communications Manager Administration Guide*.
All Calls	Allows a user to view a list, sorted in chronological order (oldest first), of all active calls on all of the user phone lines.	For more information, see Phone Button Template for All Calls, on page 173.
All Calls, Shared Line, Calling and Called Display Interaction	Improves the user experience by presenting Barge, cBarge, and Conference calls as a single unified session.	No configuration required.
All Calls on Primary Line	Allows the primary line to assume the All Calls functionality. Moving the All Calls functionality to the Primary Line frees up the feature key for other dedicated tasks.	For more information, see *Cisco Unified Communications Manager Administration Guide*.

Feature	Description	Configuration Reference
Anonymous Call Block	Allows a user to reject calls from anonymous callers.	For more information, see "SIP Profile Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*.
Any Call Pickup	Allows users to pick up a redirected call via the CTI application, on any line in their call pickup group, regardless of how the call routed to the phone.	For more information, see the "Call Pickup" chapter in *Cisco Unified Communications Manager Features and Services Guide*.
Answer (oldest call)	Allows a user to answer the oldest call that is available on all line appearances on the user phone, including Hold Reversion and Park Reversion calls that are in an altering state.	No configuration required other than to make this a programmable feature button.
Assisted Directed Call Park	Lets the end user press only one button to direct-park a call. Requires that you configure a BLF Directed Call Park button. Then, when the user presses an idle BLF Directed Call Park feature button for an active call, the active call is immediately parked at the Dpark slot that associates with the Directed Call Park feature button.	For more information, see the *Cisco Unified Communications Manager Features and Services Guide*, "Configuring Directed Call Park" chapter.
Assured Services for SIP Lines	Offers users the following enhancements: • A highly secure call flow for Cisco IP Phones and third-party telephones. • The option to place priority calls and, if necessary, preempt lower-priority phone calls through the use of Multilevel Precedence and Preemption (MLPP) service and DSCP tagging. • Support for Conference Factory on third-party phones. This feature uses Transport Layer Security (TLS) and Secure Real-time Transport Security (SRTP) protocols to ensure security on Cisco and third-party phones. The feature also introduces Early Offer and V.150 capability for Cisco and third-party phones.	For more information, see Assured Services for SIP Lines, on page 191.

Feature	Description	Configuration Reference
Audio-Only Lock Icon	Controls the display of the Security icons on the call. When the Override BFCP Application Encryption Status parameter is enabled, the Security icon displays based on the status of the audio call only. When the audio stream is encrypted, the Lock icon displays, even if the video stream is unencrypted. When the Override BFCP Application Encryption Status parameter is disabled, the Secure icon display depends on the setting of the Ignore BFCP Applications Encryption parameter. The Ignore BFCP Applications Encryption parameter controls the display of the Secure icon for the audio and video calls. The default for the Override BFCP Application Encryption Status parameter is Disabled.	For more information, see the Cisco Unified Communications Manager documentation.
AutoAnswer	Connects incoming calls automatically after a ring or two. AutoAnswer works with either the speakerphone or the headset.	For more information, see “Directory Number Configuration” chapter in the *Cisco Unified Communications Manager Administration Guide*.
Auto Dial	Allows the phone user to choose from matching numbers in the Placed Calls log while dialing. To place the call, the user can choose a number from the Auto Dial list or continue to enter digits manually.	No configuration required.

Feature	Description	Configuration Reference
Automatic Port Synchronization	When the Cisco Unified Communications Manager administrator uses the Remote Port Configuration feature to set the speed and duplex function of an IP Phone remotely, loss of packets can occur if one port is slower than the other. The Automatic Port Synchronization feature synchronizes the ports to the lower speed among the two ports, which eliminates packet loss. When automatic port synchronization is enabled, we recommend that both ports be configured for autonegotiate. If one port is enabled for autonegotiate and the other is at a fixed speed, the phone synchronizes to the fixed port speed. **Note** If both ports are configured for fixed speed, the Automatic Port Synchronization feature is ineffective. **Note** The Remote Port Configuration and Automatic Port Synchronization features are compatible only with IEEE 802.3AF Power of Ethernet (PoE) switches. Switches that support only Cisco Inline Power are not compatible. Enabling this feature on phones that are connected to these types of switches could result in loss of connectivity to Cisco Unified Communications Manager, if the phone is powered by PoE.	For more information, see Set Up Automatic Port Synchronization, on page 184.
Barge	Allows a user to join a nonprivate call on a shared phone line. The feature adds a user to a call and converts the call into a conference, allowing the user and other parties to access conference features. **Note** The Cisco Unified IP Phone can still use Barge when the Built in Bridge Enable service parameter is set to off. To prevent a user from using the Barge feature on the Cisco Unified IP Phone, you must disable Barge in Feature Control Policy for the phone.	For more information, see: • *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Configuration" chapter • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phone" chapter • *Cisco Unified Communications Manager Features and Services Guide*, "Barge and Privacy" chapter • *Cisco Unified Communications Manager Administration Guide*, "Feature Control Policy Configuration"

Feature	Description	Configuration Reference
Bluetooth Profiles	Allows you to select the Bluetooth profiles for Cisco Unified Phones 9951 and 9971. The two profiles are: • Handsfree • Human Interface Device	For more information, see Set up Bluetooth profiles, on page 184 and the *Cisco Unified Communications Manager Administration Guide*.
Block External to External Transfer	Prevents users from transferring an external call to another external number.	For more information, see "External Call Transfer Restrictions" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.
Busy Lamp Field (BLF)	Allows a user to monitor the call state of a directory number that associates with a speed-dial button, call log, or directory listing on the phone.	For more information, see "Presence" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.
Busy Lamp Field (BLF) Pickup	Provides enhancements to BLF speed dial. Allows you to configure a Directory Number (DN) that a user can monitor for incoming calls. When the DN receives an incoming call, the system alerts the monitoring user, who can then pick up the call.	For more information, see "Call Pickup" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.
Call Back	Provides users with an audio and visual alert on the phone when a busy or unavailable party becomes available.	For more information, see: • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phone" chapter • *Cisco Unified Communications Manager Features and Services Guide*, "Cisco Call Back" chapter
Call Chaperone	Allows an authorized Call Chaperone user to supervise and record a call. **Note** Control feature is configured. For more information, see the External Call Control entry in this table. The Call Chaperone user intercepts and answers the call from the calling party, manually creates a conference to the called party, and remains on the conference to supervise and record the call. Cisco Unified IP Phones with the Call Chaperone feature configured on them display a Record softkey. The Call Chaperone user presses the Record softkey to record a call. For chaperoned calls, an announcement plays or is spoken by one of the participants at the start of the call. An announcement alerts later call participants that the call is being recorded.	For more information, see the "External Call Control" chapter in *Cisco Unified Communications Manager Features and Services Guide*.

Feature	Description	Configuration Reference
Call Display Restrictions	Determines the information that displays for calling or connected lines, depending on the parties who are involved in the call.	For more information, see: • *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Configuration" chapter • *Cisco Unified Communications Manager Features and Services Guide*, "Call Display Restrictions" chapter
Call Forward	Allows users to redirect incoming calls to another number. Call forward options include Call Forward All, Call Forward Busy, Call Forward No Answer, and Call Forward No Coverage. Call forward options can be assigned on a per-line basis.	For more information, see: • *Cisco Unified Communications Manager Administration Guide*, "Directory Number Configuration" chapter • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phone" chapter • Customize User Options Web Page Display, on page 183
Call Forward All Loop Breakout	Detects and prevents Call Forward All loops. When a Call Forward All loop is detected, the Call Forward All configuration is ignored and the call rings through.	For more information, see "Cisco Unified IP Phone" chapter in the *Cisco Unified Communications Manager System Guide*.
Call Forward All Loop Prevention	Prevents a user from configuring a Call Forward All destination directly on the phone that creates a Call Forward All loop or that creates a Call Forward All chain with more hops than the existing Forward Maximum Hop Count service parameter allows.	For more information, see "Cisco Unified IP Phone" chapter in the *Cisco Unified Communications Manager System Guide*.
Call Forward Destination Override	Allows you to override Call Forward All (CFA) in cases where the CFA target places a call to the CFA initiator. This feature allows the CFA target to reach the CFA initiator for important calls. The override works whether the CFA target phone number is internal or external.	For more information, see "Understanding Directory Numbers" chapter in the *Cisco Unified Communications Manager System Guide*.
Call Forward Notification	Allows you to configure the information that the user sees upon receiving a forwarded call.	For more information, see Call Forward Notification Setup, on page 185.
Call History Display Enhancement	Displays only the call history of a selected line.	For more information, see Enable Call History Display Enhancement, on page 198.

Feature	Description	Configuration Reference
Call History for Shared Line	Allows the user to view shared line activity in the phone's call logs. This feature: • Logs missed calls for a shared line • Logs all answered and placed calls for a shared line	For more information, see Enable Call History for Shared Line, on page 189.
Call ID Display Consistency for cBarge Across Shared Line	Displays the same call ID on all calls participating in a conference call initiated on a shared line using cBarge.	No configuration required.
Call Park	Allows users to park (temporarily store) a call and then retrieve the call by using another phone in the Cisco Unified Communications Manager system.	For more information, see "Call Park and Directed Call Park" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.
Call Pickup	Allows a user to answer a call that is ringing on another phone in the pickup group by redirecting the call. You can configure the Call Pickup feature to allow a user to answer a call that is ringing: • On another phone within the pickup group. • On a particular directory number. • On a directory number in another group. • On a phone in another group that is associated with their own group. You can configure the phone to allows a user to use one-touch pickup functionality for call pickup features. You can configure audio and visual alerts for the primary line on the phone. These alerts notify the users that a call is ringing in the pickup group.	For more information, see "Call Pickup" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

Feature	Description	Configuration Reference
Call Recording	Allows a supervisor to record an active call. The user might hear a recording audible alert tone during a call when it is being recorded. When a call is secured, the security status of the call displays as a lock icon on Cisco Unified IP Phones. The connected parties might also hear an audible alert tone that indicates the call is secured and is being recorded. The Intercom feature is disabled when a call is being monitored or recorded. When an active call is being monitored or recorded, you can receive or place intercom calls; however, if you place an intercom call, the active call is put on hold, which causes the recording session to terminate and the monitoring session to suspend. To resume the monitoring session, the party whose call is being monitored must resume the call.	For more information, see the "Monitoring and Recording" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.
Call Waiting	Indicates (and allows users to answer) an incoming call that rings while on another call. Displays incoming call information on the phone screen.	For more information, see "Understanding Directory Numbers" chapter in the *Cisco Unified Communications Manager System Guide*.
Caller ID	Displays caller identification, such as a phone number, name, or other descriptive text, on the phone screen.	For more information, see: • *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Configuration" chapter • *Cisco Unified Communications Manager System Guide*, "Understanding Route Plans" chapter • *Cisco Unified Communications Manager Features and Services Guide*, "Call Display Restrictions" chapter • *Cisco Unified Communications Manager Administration Guide*, "Directory Number Configuration" chapter

Feature	Description	Configuration Reference
Caller ID Blocking	Allows a user to block their phone number or e-mail address from phones that have caller identification enabled.	For more information, see: • *Cisco Unified Communications Manager System Guide*, "Understanding Route Plans" chapter • *Cisco Unified Communications Manager Administration Guide*, "Directory Number Configuration" chapter
Calling Party Normalization	Globalizes or localizes the incoming calling party number so that the appropriate calling number presentation displays on the phone. Supports the international escape character +.	For more information, see "Calling Party Normalization" chapter in the *Cisco Unified Communications Features and Services Guide*.
CAST for SIP	Establishes communication between Cisco Unified Video Advantage (CUVA) and the Cisco Unified IP Phones to support video on the PC even on IP phones that do not have video capability.	For more information, see the *Cisco Unified Communications Manager Features and Services Guide*.
CGI CallInfo and LineInfo	Provides phone information that can be used for troubleshooting phone problems. Web access must be enabled on the phone to view the information.	No configuration required. For more information, see Request information from phone in XML, on page 262.
CGI ModelInfo	Provides phone information that can be used for troubleshooting phone problems. Web access must be enabled on the phone to view the information. A user must be associated with the phone.	No configuration required. For more information, see Request information from phone in XML, on page 262.
Cisco Extension Mobility	Allows users to temporarily access their Cisco Unified IP Phone configuration, such as line appearances, services, and speed dials, from a shared Cisco Unified IP Phone by logging into the Cisco Extension Mobility service on that phone. Cisco Extension Mobility can be useful if users work from a variety of locations within your company or if they share a workspace with coworkers.	For more information, see "Cisco Extension Mobility" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

Feature	Description	Configuration Reference
Cisco Extension Mobility Change PIN	Enables a user to change the PIN from a Cisco Unified IP Phone. The PIN can be changed by: • Using the ChangePIN softkey on the Extension Mobility logout screen. • Configuring the Change Credential IP Phone Service on the phone.	For more information, see "Cisco Extension Mobility" chapter in the *Cisco Unified Communications Manager Features and Services Guide*. For changing the PIN by using the Change Credential service, see "Configuring the Change Credential IP Phone Service" section in the *Cisco Unified Communications Manager Administration*.
Cisco Extension Mobility Cross Cluster	Enables a user configured in one cluster to sign into a Cisco Unified IP Phone in another cluster. Users from a home cluster sign into a Cisco Unified IP Phone at a visiting cluster. Configure Cisco Extension Mobility on Cisco Unified IP Phones before you configure EMCC.	For more information, see the "Cisco Extension Mobility Cross Cluster" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.
Cisco IP Manager Assistant (IPMA)	Provides call routing and other call management features to help managers and assistants handle phone calls more effectively. IPMA supports two modes of operation: proxy line support and shared line support. Both modes support multiple calls per line for the manager. The IPMA service supports both proxy line and shared line support in a cluster.	For more information, see: • *Cisco Unified Communications Manager Administration Guide* • *Cisco Unified Communications Manager Features and Services Guide*
Cisco Unified Communications Manager Express (Unified CME) Version Negotiation	The Cisco Unified Communication Manager Express uses a special tag in the information sent to the phone to identify itself. This tag enables the phone to provide services to the user that the switch supports.	For more information, see: • *Cisco Unified Communications Manager Express System Administrator Guide* • Cisco Unified IP Phone and Cisco Unified Communications Manager Express Interaction, on page 43
Cisco VXC VPN	Provides integrated VPN functionality for Cisco Virtualization Experience Clients (Cisco VXC) 2111 and 2112.	For more information, see Cisco VXC VPN Setup, on page 203.
Cisco Web Dialer	Allows users to make calls from web and desktop applications.	For more information, see "Cisco Web Dialer" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

Feature	Description	Configuration Reference
Client Matter Code	When enabled, requires a user to enter a code to identify that the call relates to a specific client matter.	For more information, see Client Matter Codes Setup, on page 185 and the "Route Pattern Configuration" section of the *Cisco Unified Communications Manager Administration Guide*.
Conference	Allows a user to talk simultaneously with multiple parties by calling each participant individually. Allows a noninitiator in a standard (ad hoc) conference to add or remove participants. Allows users to join two or more calls that are on one line to create a conference call and remain on the call. The service parameter, Advance Adhoc Conference, (disabled by default in Cisco Unified Communications Manager Administration), allows you to enable these features. **Note** Be sure to inform your users whether these features are activated.	For information about conferences, see "Conference Bridges" chapter in the *Cisco Unified Communications Manager System Guide*. For more information, go to the "Cisco Unified IP Phone" chapter in the *Cisco Unified Communications Manager System Guide*.
Conference and Transfer Enhancement	Enables conference and transfer actions to use the Simplified New Call Window or the New Call Window, depending on the setting of the Simplified New Call UI field.	For more information, see *Cisco Unified Communications Manager Administration Guide.*
Confidential Access Level (CAL)	Controls whether a call can be completed based on the CAL configuration in the Cisco Unified Communications Manager. When CAL is enabled, the user sees information about the call in a CAL message. The phone displays the CAL message for the duration of the call. If a call fails due to an incompatible CAL, the phone displays a failure message. You set up the failure message that the user sees.	For more information, see *Cisco Unified Communications Manager Administration Guide.*

Feature	Description	Configuration Reference
Configurable DF Bit	Controls how network packets are sent. Packets can be sent in chunks (fragments) of various sizes. When the DF bit is set to 1 in the packet header, the network payload does not fragment when going through network devices, such as switches and routers. Removing fragmenting avoids incorrect parsing on the receiving side, but results in slightly slower speeds. By default, the DF bit is set to 0. The bit is set in the following screens: • **System** > **Enterprise Phone** • **Device** > **Device Settings** > **Common Phone Profile** • **Device** > **Phone** The DF bit setting does not apply to ICMP, VPN, VXC VPN, or DHCP traffic.	For more information, see the Cisco Unified Communications Manager documentation.
Configurable Font Size	Allows users to increase or decrease the maximum number of characters the IP phone displays for Call History and Call Screen by changing the font size. A smaller font increases the maximum number of displayed characters, and a larger font decreases the maximum number of displayed characters.	No configuration required.
Configurable RTP/sRTP Port Range	Provides a configurable port range (2048 to 65535) for Real-Time Transport Protocol (RTP) and secure Real-Time Transport Protocol (sRTP). The default RTP and sRTP port range is 16384 to 32764. You configure the RTP and sRTP port range in the SIP Profile.	For more information, see Set up RTP/sRTP port range, on page 200
Configurable TLS Session Resumption Timer	Enables resumption of TLS handshake without repeating the authentication or confidentiality or authorization process. The TLS resumption timer range is between 0 to 3600 sec and the default timer value is 3600 sec.	For more information, see TLS Session Resumption Timer, on page 201.
CTI Applications	A computer telephony integration (CTI) route point can designate a virtual device to receive multiple, simultaneous calls for application-controlled redirection.	For more information, see “CTI Route Point Configuration” chapter in the *Cisco Unified Communications Manager Administration Guide*.

Feature	Description	Configuration Reference
CTL and ITL Status Display and Report	Enables you to report the CTL and ITL information to the Cisco Unified Communications Manager, using a Cisco Unified IP Phone.	For more information, see the *Cisco Unified Communications Manager Administration Guide*.
Custom Line Filters	Enables users to set the alerting call notification priority on a subset of lines covered by an alert filter. The custom filter generates either traditional pop-up alerts or actionable alerts for incoming calls on the selected lines. For each filter, only the subset of lines under coverage will generate an alert. If a filter is turned off, lines under its coverage will not show alert notifications. You can configure or edit the default phone filter. If configured, the default phone filter is displayed to the user as the Daily schedule filter.	For more information, see Custom Line Filter Setup, on page 198.
Default Back To All Calls	Improves the experience for users with multiple lines by displaying the primary line with the All Calls view when a call completes. To have a phone return to the primary line with the All Calls filter view active, you must enable both the Show All Calls on Primary Line and the Revert to All Calls features.	For more information, see *Cisco Unified Communications Manager Administration Guide*.
Default Wallpaper Control	When the Enable End User Access to Phone Background Image Setting check box is enabled, users can change the background image (or wallpaper) for the LCD screen on their phone. When the Enable End User Access to Phone Background Image Setting check box is disabled, users cannot change the background image on the phone.	For more information, see the "Common Phone Profile Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*.
Device Invoked Recording	Provides end users with the ability to record their telephone calls via a softkey. In addition, administrators may continue to record telephone calls via the CTI User Interface.	For more information, see Enable Device Invoked Recording, on page 189.
Dial Tone From Release Key	Allows users to disconnect a call and get the dial tone by pressing only one button. When the user presses the Release button while on a call or while dialing off-hook, the active call ends and dial tone sounds. The New Call window appears on the selected line on the phone screen.	For more information, see Dial Tone from Release Button Setup, on page 193.

Feature	Description	Configuration Reference
Directed Call Park	Allows a user to transfer an active call to an available directed call park number that the user dials or speed dials. A Call Park BLF button indicates whether a directed call park number is occupied and provides speed-dial access to the directed call park number.	For more information, see "Call Park and Directed Call Park" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.
Divert	Allows a user to transfer a ringing, connected, or held call directly to a voice-messaging system or to the busy target. Divert acts on the highlighted call only. Incoming calls are not automatically highlighted. If a second call rings while the user is on the first call, Divert acts on the first call unless the user actively highlights the second call. When a call is diverted, the line becomes available to make or receive new calls. When Enhanced Immediate Divert is enabled, it allows users to transfer incoming calls directly to their voice messaging system or to the voice messaging system of the original called party.	For more information about diverting calls to voicemail, see "Immediate Divert" chapter in the *Cisco Unified Communications Manager Features and Services Guide*. For more information about Enhanced Immediate Divert, see "Cisco Unified IP Phone" chapter in the *Cisco Unified Communications Manager System Guide*.
Dual Bank Information	Allows the Cisco Unified Communications Manager administrator to upgrade phone firmware with a new load before resetting the previous load to an Inactive load status. The Cisco Unified Communications Manager administrator can verify whether the active and inactive loads were swapped correctly.	For more information, see Set Up Dual Bank Information, on page 186.

Feature	Description	Configuration Reference
Do Not Disturb (DND)	When DND is turned on, either no audible rings occur during the ringing-in state of a call, or no audible or visual notifications of any type occur. You can configure the phone with a phone-button template with DND as one of the selected features. The following DND-related parameters are configurable in Cisco Unified Communications Manager Administration: • Do Not Disturb: This check box allows you to enable DND on a per-phone basis. Use the Phone Configuration window in **Cisco Unified Communications Manager Administration** > **Device** > **Phone**. • DND Incoming Call Alert: Choose the type of alert, if any, to play on a phone for incoming calls when DND is active. This parameter is located on both the Common Phone Profile window and the Phone configuration window. The phone Configuration window value takes precedence. • BLF Status Depicts DN: Enables DND status to override busy/idle state.	For more information, see "Do Not Disturb" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.
Enable Video On/Off	Improves the video conference call flow by removing the black box that is displayed when one party has the Auto Transmit setting on their phone set to Off. Supported on Cisco Unified IP Phones 9951 and 9971. Not supported on Cisco Unified IP Phone 8961.	For additional information, see Enable Video On/Off Setting, on page 193 .
EnergyWise	Enables an IP Phone to sleep (power down) and wake (power up) at predetermined times, to promote energy savings	For more information, see EnergyWise on the Cisco Unified IP Phone Setup, on page 219.
Enhanced Secure Extension Mobility Cross Cluster	Improves the Secure Extension Mobility Cross Cluster (EMCC) feature by preserving the network and security configurations on the login phone. Doing so maintains security policies, preserves network bandwidth, and avoids network failure within the visiting cluster (VC).	For more information, see *Cisco Unified Communications Manager Features and Services Guide*.
Enlarge Unique Call Identifier	The unique call identifier displays at the same font size as the calling number.	No configuration required.
E-SRST Enhancements	Enables Video, Shared Line, and BLF Speed Dial in SRST mode. For more information, see Survivable Remote Site Telephony, on page 162.	No configuration required.

Feature	Description	Configuration Reference
External Call Control	Allows Cisco Unified Communications Manager to route audio and video calls to a route server that hosts routing rules. The route server receives routing requests from Cisco Unified Communications Manager and in turn returns routing directives to Cisco Unified Communications Manager.	For more information, see the "External Call Control" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.
Fast Dial Service	Allows a user to enter a Fast Dial code to place a call. You can assign Fast Dial codes to phone numbers or to Personal Address Book entries. (See "Services" in this table.)	For more information, see Phone Button Template for Personal Address Book or Speed Dials, on page 174.
FIPS 140-2 Level 1	Federal Information Processing Standard (FIPS) 140-2 Level 1 provides a secure, encrypted environment that meets the United States Department of Defence Unified Capabilities Requirements (UCR) 2008 standard. The default setting is Disable.	For more information, see Product-Specific Configuration, on page 165.
Forced Authorization Code	Requires a user to enter an authorization code to place a call. Controls the types of calls that certain users can place.	For more information, see Forced Authorization Codes Setup, on page 187 and the "Route Pattern Configuration" section of the *Cisco Unified Communications Manager Administration Guide*.
Gateway Recording For SIP	Provides the ability to record calls using Cisco Voice Gateway. This allows you to record calls made on Cisco Jabber, a Cisco IP Phone (SIP), or calls made on a mobile device.	For more information, see *Cisco Unified Communications Manager Features and Services Guide*.
Handset Bass Adjustment	Allows a user to set the phone to use either a reduced bass tone or the full bass tone. Reduced bass removes low frequencies, which can improve muffled voices or insufficient volume on handsets. The default setting is for reduced bass.	No configuration required.

Feature	Description	Configuration Reference
Headset Sidetone Controls	Allows you to adjust headset levels to one of five following settings: • Off • Very Low • Low • Normal • boost **Note** This feature is only for analog headsets.	For more information, see the following: • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phone" chapter. • *Cisco Unified Communications Manager Administration Guide*, "Setting Headset Sidetone Controls" section
Hide Softkeys in Full Screen Video Mode	Controls the way that softkeys display in full screen video mode.	No configuration required
Hide Video Option	Provides flexibility with the flexibility to hide the video window. When the video is displayed, the user sees the Hide Video softkey; when the video is hidden, the user sees the Show Video softkey. The phone supports a new configuration parameter that enables the administrator to control whether the video is displayed or hidden. The parameter is Hide Video By Default, with values Disabled (default) or Enabled.	For more information, see *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones" chapter.
Hide Wi-Fi User Interface Setting	Removes the Wireless Setup option from the Network Setup menu when WiFi is disabled from the Cisco Unified Communications Manager. This feature is supported only on the Cisco Unified IP Phone 9971.	For more information, see the "Cisco Unified IP Phone Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*.
Hold Reversion	Limits the amount of time that a call can be on hold before it reverts back to the phone that put the call on hold and alerts the user. Reverting calls are distinguished from incoming calls by a single ring (or beep, depending on the new call indicator setting for the line). This notification repeats at intervals if the call is not resumed. A call that triggers Hold Reversion also displays an animated icon in the call bubble and a brief message on the status line. You can configure call focus priority to favor incoming or reverting calls.	For more information about configuring this feature, see "Hold Reversion" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.
Hold Status	Enables phones with a shared line to distinguish between the local and remote lines that placed a call on hold.	No configuration required.

Feature	Description	Configuration Reference
Hold/Resume	Allows the user to move a connected call from an active state to a held state. To place a call on hold, press the Hold button. To resume a call, choose the line with the held call and press Resume.	No configuration required unless you want to use music on hold. See the "Music on Hold" entry in this table for information. See also the "Hold Reversion" entry in this table.
Hold/Resume Toggle	Allows you to toggle a call between an active state and on-hold state using the Hold button. To place a call on hold, press Hold. To resume the call, press Hold again.	The hard key for this feature requires no configuration. For more information, see "Hold Reversion" in this table. To enable a caller to hear music while on hold, see "Music on Hold" in this table.
Hunt Group Display	Provides load sharing for calls to a main directory number. A hunt group contains a series of directory numbers that can answer the incoming calls. When an incoming call is offered to a directory number that is part of the hunt group, this feature displays the main directory number in addition to the calling party.	For more information, see: • *Cisco Unified Communications Manager Administration Guide*, "Hunt Group Configuration" chapter • *Cisco Unified Communications Manager System Guide*, "Understanding Route Plans" chapter • *Cisco Unified Communications Manager Administration Guide*, "CTI Route Point Configuration" chapter
Incoming Call Toast Timer	Allows you to set the length of time that an incoming call toast (notification) appears on the phone screen.	For more information, see Incoming Call Toast Timer Setup, on page 187.
Intercom	Allows users to place and receive intercom calls using programmable phone buttons. You can configure intercom line buttons to: • Directly dial a specific intercom extension. • Initiate an intercom call and then prompt the user to enter a valid intercom number. **Note** If your user logs into the same phone on a daily basis with their Cisco Extension Mobility profile, assign the phone button template that contains intercom information to their profile, and assign the phone as the default intercom device for the intercom line. **Note** The Intercom feature does not support Extension Mobility Cross Cluster.	For more information, see "Intercom" chapter in the *Cisco Unified Communications Manager Feature and Services Guide*.

Feature	Description	Configuration Reference
Intelligent Session Control	Reroutes an enterprise originated call that was placed a user's mobile phone through the enterprise number. The call only rings the user mobile but not the desk phone. When the user answers the call on the mobile phone, the desk phone displays a Remote in Use message. During these calls, a user can use the various features of the mobile phone.	For more information, see "Cisco Unified Mobility" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.
IPv6 Support	Provides support for expanded IP addressing on Cisco IP Phones. IPv6 support is provided in standalone or in dual-stack configurations. In dual-stack mode, the phone is able to communicate using IPv4 and IPv6 simultaneously, independent of the content.	For more information, see IPv6.
Line Select	If this feature is disabled (default), the ringing line is selected. When the feature is enabled, the primary line is picked up even if a call is ringing on another line. The user must manually select the other line. **Note** This feature can also be enabled or disabled for Extension Mobility.	For more information, see the option "Always use prime line" in the following chapters of the *Cisco Unified Communications Manager Administration Guide*: • "Device Profile Configuration" • "Common Phone Profile Configuration" • "Cisco Unified IP Phone Services Configuration"
Line Select for Voice Messages	When disabled (default), pressing the Messages button selects the line that has a voice message. If more than one line has voice mail, the first available line is selected. When the features is enabled, the primary line is always used to retrieve voice messages. **Note** This feature can also be enabled or disabled for Extension Mobility.	For more information, see the option "Always use prime line for voice message" in the following chapters of the *Cisco Unified Communications Manager Administration Guide*: • "Device Profile Configuration" • "Common Phone Profile Configuration" • "Cisco Unified IP Phone Services Configuration"
Line State Display Enhancement	Enables users to see if a Cisco Unified IP Phone is in the Remote-in-use state when there is a call alert on shared lines.	For more information, see *Cisco Unified Communications Manager Administration Guide*.

Feature	Description	Configuration Reference
Line Status for Call Lists	Allows the user to see the Line Status availability status of monitored line numbers in the Call History list. The Line Status states are: • Unknown • Idle • Busy • DND	For more information, see Enable Line Status for Call Lists, on page 186.
Log Out Of Hunt Groups	Allows users to sign out of a hunt group and temporarily block calls from ringing their phone when they are not available to take calls. Logging out of hunt groups does not prevent non-hunt group calls from ringing their phone.	For more information, see • Services Setup, on page 180 • *Cisco Unified Communications Manager System Guide*, "Understanding Route Plans" chapter
Malicious Caller Identification (MCID)	Allows users to notify the system administrator about suspicious calls.	For more information, see: • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phone" • *Cisco Unified Communications Manager Features and Services Guide*, "Malicious Call Identification" chapter
Meet Me Conference	Allows a user to host a Meet Me conference in which other participants call a predetermined number at a scheduled time.	For more information, see "Meet-Me Number/Pattern Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*.
Message Waiting	Defines directory numbers for message waiting on and message waiting off indicators. A directly connected voice-messaging system uses the specified directory number to set or to clear a message-waiting indication for a particular Cisco Unified IP Phone.	For more information, see: • *Cisco Unified Communications Manager Administration Guide*, "Message Waiting Configuration" chapter • *Cisco Unified Communications Manager System Guide*, "Voice Mail Connectivity to Cisco Unified Communications Manager" chapter

Feature	Description	Configuration Reference
Visual Message Waiting Indicator	A light on the handset that indicates that a user has one or more new voice messages.	For more information, see: • *Cisco Unified Communications Manager Administration Guide*, "Message Waiting Configuration" chapter • *Cisco Unified Communications Manager System Guide*, "Voice Mail Connectivity to Cisco Unified Communications Manager" chapter
Message Waiting Indicator (MWI)	The MWI is both a visual indicator, viewable from 360 degrees and an audible message waiting indicator. Users change the voice message light on their handset and the audible voice message indicator on their phone by logging in to their User Options web pages and accessing the message indicator settings. Users change the setting to on or off.	For more information, see "Cisco Unified IP Phone" chapter in the *Cisco Unified Communications Manager System Guide*.
Missed Call History	Allows a user to specify whether missed calls are logged in the missed calls history for a given line appearance.	For more information, see the "Directory Number Configuration" chapter in the*Cisco Unified Communications Manager Administration Guide*.
Mobile Connect	Enables users to manage business calls by using a single phone number and pick up in-progress calls on the desktop phone and a remote device, such as on a mobile phone. Users can restrict the group of callers according to phone number and time of day. Also see the Session Handoff entry in this table.	For more information, see "Cisco Unified Mobility" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.
Mobile Voice Access	Extends Mobile Connect capabilities by allowing users to access an interactive voice response (IVR) system to originate a call from a remote device, such as a cellular phone.	For more information, see "Cisco Unified Mobility" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

Feature	Description	Configuration Reference
Monitoring and Recording	Allows a supervisor to monitor an active call silently. Neither party on the call can hear the supervisor. The user may receive an audible alert during a call when it is being monitored. When a call is secure, a lock icon displays. Callers may also receive an audible alert to indicate that the call is being monitored. The connected parties may also receive an audible alert that indicates that the call is secure and is being monitored. When an active call is being monitored or recorded, the user can receive or place intercom calls; however, if the user places an intercom call, the active call is put on hold. This action causes the recording session to terminate and the monitoring session to suspend. To resume the monitoring session, the person being monitored must resume the call.	For more information, see "Monitoring and Recording" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.
Multiple Calls Per Line Appearance	Each line can support multiple calls. Only one call can be active at any time; other calls are automatically placed on hold.	For more information, see "Understanding Directory Numbers" chapter in the *Cisco Unified Communications Manager System Guide*.
Music On Hold	Plays music while callers are on hold.	For more information, see "Music On Hold" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.
Mute	Mutes the microphone from the handset or headset.	No configuration required.
New Versions of Cisco Unified IP Phone 8961, 9951, and 9971	Provides new versions of the existing phone models. The model numbers remain the same. This feature affects all phones manufactured after October 31, 2012. These phones must run Firmware Release 9.3(2) or later. The phone firmware does not allow the phone to be downgraded to releases earlier than Release 9.3(2).	No configuration required.
On-Hook Dialing	Allows a user to dial a number without going off hook. The user can then either pick up the handset, press Call, or press either the headset or speaker buttons to initiate the call.	For more information, see the "Calling Features" chapter in the *Cisco Unified IP Phone 8961, 9951, and 9971 User Guide for Cisco Unified Communications Manager (SIP)*.
One Button Access to Call History	Provides the user with quick access to the Call History screen.	No configuration required.

Feature	Description	Configuration Reference
One Touch Private Line Automatic Ringdown (PLAR)	Improves the Private Line Automated Ringdown (PLAR) feature by automatically selecting the line for the call.	For more information, see "Directory Number Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*.
Park Monitoring	Monitors the status of a parked call. The park monitoring call bubble is not cleared until the parked call gets retrieved or is abandoned by the parkee. This parked call can be retrieved by using the same call bubble on the parker phone.	For more information, see Park Monitoring, on page 194. For information about call park, see the "Call Park and Directed Call Park" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.
Pause In Speed Dial	Users can set up the speed-dial feature to reach destinations that require Forced Authorization Code (FAC) or Client Matter Code (CMC), dialing pauses, and additional digits (such as a user extension, a meeting access code, or a voicemail password) without manual intervention. When the user presses the speed dial, the phone establishes the call to the specified DN and sends the specified FAC, CMC, and DTMF digits to the destination and inserts the necessary dialing pauses.	For more information, see Pause in Speed Dial, on page 190.
Peer Firmware Sharing	Provides the following advantages in high-speed campus LAN settings: • Limits congestion on TFTP transfers to centralized remote TFTP servers • Eliminates the need to manually control firmware upgrades • Reduces phone downtime during upgrades when large numbers of devices are reset simultaneously Peer Firmware Sharing may also aid in firmware upgrades in branch/remote office deployment scenarios that run over bandwidth-limited WAN links.	For more information, see Set Up Peer Firmware Sharing, on page 187.
Phone Secure Web Access	Cisco Unified IP Phones can securely access the web with the use of a phone trust store called "phone-trust."	For more information, see the "Security Overview" chapter in the *Cisco Unified Communications Manager Security Guide*.
Plantronics Blackwire C220 USB Headset	The phones support this headset.	For more information, see USB Headsets, on page 61.
PLK Support For Queue Statistics	Enables the users to query the call queue statistics for hunt pilots and the information appears on phone screen.	For more information, see Feature Buttons and Softkeys, on page 171

Feature	Description	Configuration Reference
Plus Dialing	Allows the user to dial E.164 numbers that are prefixed with a "+" sign. To dial the + sign, the user needs to press and hold the "*" key for at least 1 second. This applies to dialing the first digit for an on-hook or off-hook call only.	No configuration required.
Power Negotiation over LLDP	Allows the phone to negotiate power using LLDP and CDP protocols. Power Negotiation should not be disabled when the phone is connected to a switch that supports power negotiation. If disabled, it could cause the switch to shut off power to the phone. The Power Negotiation feature is enabled by default. To change the setting of Power Negotiation to Disabled, select Disabled in the Power Negotiation drop-down list in the Product Specific Configuration area of the Phone Configuration window (**Device** > **Phone**).	For more information, see *Cisco Unified Communications Manager Administration Guide*.
Presence-Enabled Directories	Allows a user to monitor the call state of another directory number (DN) that is listed in call logs, speed dials, and corporate directories. The Busy Lamp Field (BLF) for the DN displays the call state.	For more information, see "Presence" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.
Privacy	Prevents users who share a line from adding themselves to a call and from viewing information on their phone screens about the call of another user.	For more information, see: • *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Configuration" chapter • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phone" chapter • *Cisco Unified Communications Manager Features and Services Guide* "Barge and Privacy" chapter
Private Line Automated Ringdown (PLAR)	The Cisco Unified Communications Manager administrator can configure a phone number that the Cisco Unified IP Phone dials as soon as the handset goes off hook. This feature can be useful for phones that are designated for calling emergency or "hotline" numbers.	For more information, see "Directory Number Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*.

Feature	Description	Configuration Reference
Programmable Feature Button	The administrator can assign features to programmable keys. When the administrator configures features on a feature button, the features always remain visible and accessible to the user; for example, the administrator can assign a dedicated Pickup button on the phone.	For more information, see: • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phone" chapter • *Cisco Unified Communications Manager Administration Guide*, "Phone Button Template Configuration" chapter
Prompt for Barge	Provides an option to display a visual alert prompt when a user tries to barge into a call. This feature is configured on the phone by the user in **Settings** > **Preferences** > **Barge Alert**. By default, the Barge Alert option is set to Off and the user can barge into an eligible shared lined without receiving a prompt. When Barge Alert is set to On, an alert displays and the user must confirm the barge.	No configuration required.
Protected Calling	Provides a secure (encrypted) connection between two phones. A security tone plays at the beginning of the call to indicate that both phones are protected. Some features, such as conference calling, shared lines, Extension Mobility, and Join Across Lines are not available when protected calling is configured. Protected calls are not authenticated.	For more information about security, see Supported security features, on page 28. For more information, see *Cisco Unified Communications Manager Security Guide*.
Quality Reporting Tool (QRT)	Allows users to use Report Quality on a phone to submit information about problem phone calls. QRT can be configured for either of two user modes, depending upon the amount of desired user interaction with QRT.	For more information, see: • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phone" chapter • *Cisco Unified Communications Manager Features and Services Guide*, "Quality Report Tool" chapter
Redial	Allows users to call the most recently dialed phone number by pressing Redial.	No configuration required.

Feature	Description	Configuration Reference
Remote Port Configuration	Allows the administrator to configure the speed and duplex function of the phone Ethernet ports remotely by using Cisco Unified Communications Manager Administration. This practice enhances the performance for large deployments with specific port settings. **Note** If the ports are configured for Remote Port Configuration in Cisco Unified Communications Manager Administration, the data cannot be changed on the phone.	For more information, see Remote Port Configuration Setup, on page 188.
Ring Tone Setting	Identifies ring type that is used for a line when a phone has another active call.	For more information, see: • *Cisco Unified Communications Manager Administration Guide*, "Directory Number Configuration" chapter • Custom phone rings, on page 212
Ringtone	Users can customize how their phone indicates an incoming call and a new voice mail message.	For more information, see "Custom Phone Rings" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.
RTCP Always On	Simplifies the phone administration by removing the need to set the RTCP Control for Video field. RTCP is always turned on for phones.	No configuration required.
RTCP Control For Video	The administrator can enable the phones to transmit and receive RTCP packets for both audio and video streams in a video call. Configure the RTCP for video parameter from the Phone Configuration or Common Phone Profile Configuration window in Cisco Unified Communications Manager Administration.	For more information, see the *Cisco Unified Communications Manager Administration Guide*.
RTCP Hold For SIP	Ensures that the gateway does not drop held calls. The gateway checks the status of the RTCP port to determine whether a call is active or not. By keeping the phone port open, the gateway will not end held calls.	No configuration required.
Secure and Nonsecure Indication Tone	Controls the playing of the Secure indication tone. For more information, see Secure and nonsecure call indication tone, on page 165.	No configuration required.

Feature	Description	Configuration Reference
Secure Extension Mobility Cross Cluster	Enables a user in one cluster (using an encrypted/authenticated Cisco Unified IP Phone with TFTP Encrypted Config/Digest Authentication enabled) to log in to another cluster when two cluster are both in mixed mode.	For more information, see the "Cisco Extension Mobility Cross Cluster" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.
Secure Conference	Allows secure phones to place conference calls by using a secured conference bridge. As new participants are added by using the Confrn or Barge softkeys or MeetMe conferencing, the secure call icon displays as long as all participants use secure phones. The Conference List displays the security level of each conference participant. Initiators can remove nonsecure participants from the Conference List. (Noninitiators can add or remove conference participants if the Advanced Adhoc Conference Enabled parameter is set.)	For more information about security, see Supported security features, on page 28. For more information, see: • *Cisco Unified Communications Manager System Guide*, "Conference Bridges" chapter • *Cisco Unified Communications Manager Administration Guide*, "Conference Bridge Configuration" chapter • *Cisco Unified Communications Manager Security Guide*
Separate Audio and Video Mute	Allows the administrator to control the user's ability to mute the audio while transmitting a video image. This feature is disabled by default.	For more information, see Set up Separate Audio and Video Mute, on page 199.
Separate Audio and Video Port Range Configuration	Enables you to improve Quality of Service (QoS) by configuring audio traffic and video traffic on different ports.	For more information, see Set up audio and video port range, on page 201.
Serviceability for SIP Endpoints	Enables administrators to quickly and easily gather debug information from phones. This feature uses SSH to remotely access each IP phone. SSH must be enabled on each phone for this feature to function.	For more information, see Enable phone debugging, on page 288.
Services	Allows you to use the Cisco Unified IP Phone Services Configuration menu in Cisco Unified Communications Manager Administration to define and maintain the list of phone services to which users can subscribe. **Note** Some services appear on the phone by default, or you can disable them so that they do not display on the phone.	For more information see: • *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Configuration" chapter • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phone Services" chapter

Feature	Description	Configuration Reference
Services URL Button	Allows users to access services from a programmable button rather than by using the Services menu on a phone.	For more information see: • *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Configuration" chapter • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phone Services" chapter
Session Handoff	Allows users to switch calls from a mobile phone to Cisco Unified devices that share the same line. Handsets on all the devices on the shared line then flash simultaneously. After a user answers the call from one of the Cisco Unified devices, the other Cisco Unified devices that share the same line display a Remote in Use message. However, if the call fails to switch from the mobile phone, the mobile phone might display a Cannot Move Conversation message.	For more information, see: • *Cisco Unified Communications Manager Features and Services Guide*, "Cisco Unified Mobility" chapter • *Cisco Unified Communications Manager Features and Services Guide*, "Cisco Unified Mobility Advantage and Cisco Unified Mobile Communicator Integration" chapter
Shared Line	Allows a user with multiple phones to share the same phone number or allows a user to share a phone number with a coworker.	For more information, see "Understanding Directory Numbers" chapter in the *Cisco Unified Communications Manager System Guide*.
Simplified New Call Bubble	Provides a new user interface for off-hook dialing. It is disabled by default. The Simplified New Call Window does not allow the user to select a number from the call history. To enable Simplified New Call in the Cisco Unified CM Administration application, navigate to the Phone Configuration window, then set the Simplified New Call UI field to Enabled.	For more information, see *Cisco Unified Communications Manager Administration Guide*.
SIP Phone No Alert Name	The SIP Phone No Alert Name feature makes it easier for end users to identify alert calls by displaying the alert name in the Placed Calls history.	No configuration required.
SSH Disable	Enables or disables the use of SSH on the phone.	For more information, see SSH Access, on page 222.
Softkey Policy Control	Enables you to configure certain features as either softkeys or programmable feature buttons.	For more information, see Enable Softkey Policy Control, on page 199.

Feature	Description	Configuration Reference
Softkey Template	Allows you to manage the softkeys on the Cisco Unified IP Phones. A maximum of 16 softkeys can be configured per template. However, the phone supports 18 softkeys per set, so that you can add two built-in softkeys to each softkey set.	For more information, see Softkey template.
Speed Dial	Allows users to speed dial a phone number by entering an assigned index code (1-99) on the phone keypad. **Note** You can use Speed Dialing while on-hook or off-hook. Users assign index codes from the User Options web pages.	For more information, see: • *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Configuration" chapter • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phone" chapter
sRTP Secure Video	The administrator can configure the RTCP authentication tag length for secure video calls. **1** Native Video supports security, but CUVA has only a nonsecure stream. **2** For secure video calls, the secure icon displays on phone screen in the top right corner if Picture in Picture (PIP) is not active. When PIP is active, the icon displays in the top left corner. **3** The RTCP authentication tag length can only be configured for the audio stream. The video stream has a default 80-bit configuration and cannot be configured.	Configure the 80-bit SRTCP field from the Phone Configuration, Common Phone Profile Configuration, or Enterprise Phone Configuration window in Cisco Unified Communications Manager Administration. For more information, see the *Cisco Unified Communications Manager Administration Guide*.
Support For Hold Button On USB Headsets	Provides support for USB headsets equipped with a Hold button. Users can put a call on hold using the headset button and retrieve the call using the Resume softkey on their phone.	No configuration required.
Support For USB Headsets	The phones support the following USB headsets: • BlackWire C220 Series • BlackWire C420 • Blackwire C620 • Savi 7xx • Voyager Pro UC v2	No configuration required.

Feature	Description	Configuration Reference
Time-of-Day Routing	Restricts access to specified telephony features by time period.	For more information, see: • *Cisco Unified Communications Manager Administration Guide*, "Time Period Configuration" chapter • *Cisco Unified Communications Manager System Guide*, "Time-of-Day Routing" chapter
Time Zone Update	Updates the Cisco Unified IP Phone with time zone changes.	For more information, see the *Cisco Unified Communications Manager Administration Guide*, "Date/Time Group Configuration" chapter.
Transfer	Allows users to redirect connected calls from their phones to another number. The user can connect two calls to each other. The user can remain on the line or transfer the call without staying on the line.	No configuration required.
Uniform Resource Identifier Dialing	The Uniform Resource Identifier (URI) Dialing feature enables the user to place calls by using an alphanumeric URI address as a directory number, for example, bob@cisco.com. The user must enter the URI address to select the contact. The phone screen displays the call information for the URI call. The call logs record the URI call information in the Call History and the Details page. **Note** The user cannot use the soft keypad to place calls by URI address.	For more information, see: • *Cisco Unified Communications Manager Features and Services Guide* • *Cisco Unified IP Phone 8961, 9951, and 9971 User Guide for Cisco Unified Communications Manager (SIP)*
Uniform Resource Identifier Dialing Enhancement	Allows you to specify the device display preference for calls that have both Directory Number (DN) and URI available. If the URI Dialing Display Preference is set to DN then DN is displayed when available. If the URI Dialing Display Preference is set to URI then URI is displayed available.	For more information, see the • *Cisco Unified Communications Manager Features and Services Guide* • *Cisco Unified IP Phone 8961, 9951, and 9971 User Guide for Cisco Unified Communications Manager (SIP)*
Unique Call ID Display	Ensures that all calls with the same group call ID display the same call ID on all the phones in the group. Displaying the same call ID on all phones ensures that group users can identify the correct active call.	No configuration required.

Feature	Description	Configuration Reference
Unique cBarge Call Instance ID	Enhances cBarge by giving the legs of the call the same Call ID.	No configuration required.
VDI VPN	Provides integrated VPN functionality for Cisco virtual desktop infrastructure (VDI) clients.	For more information, see Cisco VXC VPN, on page 202.
Video Mode	Allows a user to select the video display mode for viewing a video conference, depending on the modes that are configured in the system.	For more information, see: • *Cisco Unified Communications Manager Administration Guide*, "Conference Bridge Configuration" chapter • *Cisco Unified Communications Manager System Guide*, "Understanding Video Telephony" chapter
Video Support	Enables video support on the phone.	For more information, see: • *Cisco Unified Communications Manager Administration Guide*, "Conference Bridge Configuration" chapter • *Cisco Unified Communications Manager System Guide*, "Understanding Video Telephony" chapter • *Cisco VT Advantage Administration Guide*, "Overview of Cisco VT Advantage" chapter
VPN	Using SSL, provides a virtual private network (VPN) connection on the Cisco Unified IP Phone when it is located outside a trusted network or when network traffic between the phone and Unified Communications Manager must cross untrusted networks. **Note** This VPN is differs from VXC VPN. See the description of Cisco VXC VPN in this table.	For more information, see the "Virtual Private Networks Setup" chapter in the *Cisco Unified Communications Manager Security Guide*.

Feature	Description	Configuration Reference
Voice Messaging System	Enables callers to leave messages if calls are unanswered.	For more information, see: • *Cisco Unified Communications Manager Administration Guide*, "Cisco Voice-Mail Port Configuration" chapter • *Cisco Unified Communications Manager System Guide*, "Voice Mail Connectivity to Cisco Unified Communications Manager" chapter

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.

The following table describes the availability of features during failover.

Table 23: SRST feature support

Feature	Supported	Notes
New Call	Yes	
End Call	Yes	
Redial	Yes	
Answer	Yes	
Hold	Yes	
Resume	Yes	
Conference	Yes	
Conference to Active Calls (Join)	No	The Active Calls softkey does not display.
Conference List	No	
Transfer	Yes	

Feature	Supported	Notes
Transfer to Active Calls (Direct Transfer)	No	
Auto Answer	Yes	
Call Waiting	Yes	
Caller ID	Yes	
Audible Message Waiting Indicator	Yes	
All Calls Programmable Line Key	Yes	
Answer Programmable Line Key	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	
Service IRL Programmable Line Key	Yes	
To Voicemail (iDivert)	No	The iDivert softkey does not display.

Feature	Supported	Notes
Line Filters	Partial	Lines are supported but cannot be shared.
Park Monitoring	No	The Park softkey does not display.
Barge	No	User sees the message `That feature is not currently available.`
Enhanced Message Waiting Indication	No	Message count badges do not appear on the phone screen. Only the Message Waiting icon displays.
Directed Call Park	No	The softkey does not display.
BLF	Partial	BLF feature key works like Speed Dial keys.
Hold Reversion	No	Calls remain on hold indefinitely.
Remote Hold	No	Calls appear as Local Hold calls.
Meet Me	No	The Meet Me softkey does not display.
PickUp	No	The softkey causes no action.
Group PickUp	No	The softkey causes no action.
Other PickUp	No	The softkey causes no action.
Malicious Call ID	No	The softkey causes no action.
QRT	No	The softkey causes no action.
Hunt Group	No	The softkey causes no action.
Intercom	No	The softkey causes no action.
Mobility	No	The softkey causes no action.
Privacy	No	The softkey causes no action.
Call Back	No	The Call Back softkey does not display.
Video	Yes	Video conference is not supported.

Feature	Supported	Notes
Shared Line	Yes	
BLF Speed Dial	Yes	

Secure and nonsecure call indication tone

When a phone is configured as secure (encrypted and trusted) in 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.

Only protected phones hear these secure or nonsecure indication tones. Nonprotected phones never hear tones. If the overall call status changes during the call, the indication tone changes accordingly. At that time, the protected phone plays the appropriate tone.

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

- When the option to play the tone is enabled, Play Secure Indication Tone option is enabled (True):
  - 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 indication tone (six short beeps with brief pauses).

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

Product-Specific Configuration

Cisco Unified Communications Manager Administration allows you to set some product-specific configuration parameters for Cisco Unified IP Phones in any of the following windows:

- Phone Configuration window (**Device** > **Phone**); Product Specific Configuration portion of window
- Common Phone Profile Configuration window (**Device** > **Device Settings** > **Common Phone Profile**)
- Enterprise Phone Configuration window (**System** > **Enterprise Phone Configuration**)

Product-Specific Configuration Parameters

You can set the following parameters in any of the previously listed configuration windows:

- Back USB Port (for Cisco Unified IP Phones 9951 and 9971)
- Side USB Port
- Enable/Disable USB Classes
- Bluetooth (for Cisco Unified IP Phones 9951 and 9971)
- Bluetooth Profiles (only for Cisco Unified IP Phones 9951 and 9971)
- WLAN (for Cisco Unified IP Phone 9971 only)
- Settings Access
- Web Access
- Days Display Not Active
- Display on Time
- Display on Duration
- Display Idle Timeout
- Enable Power Save Plus
- Phone On Time
- Phone Off Time
- Phone Off Idle Timeout
- Enable Audio Alert
- EnergyWise Domain
- EnergyWise Secret
- Allow EnergyWise Overrides
- Load Server
- RTCP
- Peer Firmware Sharing
- Cisco Discovery Protocol (CDP): Switch Port
- Cisco Discovery Protocol (CDP): PC Port
- Link Layer Discovery Protocol - Media Endpoint Discover (LLDP-MED): Switch Port
- Link Layer Discovery Protocol (LLDP): PC Port
- 802.1x Authentication
- Switch Port Remote Configuration
- PC Port Remote Configuration

- Automatic Port Synchronization
- Power Negotiation
- Restrict Data Rates
- SSH Access
- Incoming Call Toast Timer
- Provide Dial Tone from Release Button
- Hide Video By Default
- Background Image
- Simplified New Call UI
- Enable VXC VPN for MAC
- VXC VPN Option
- VXC Challenge
- VXC-M Servers
- Revert to All Calls
- 80-bit SRTCP
- RTCP for Video
- Record Call Log from Shared Line
- Show Call History for Selected Line Only
- Actionable Incoming Call Alert
- DF bit
- Default Line Filter

Note Click the **?** button in Cisco Unified Communications Manager Administration for descriptions of these parameters.

Override Common Settings Check Box

When you set the parameters, check the Override Common Settings check box for each setting that you wish to update. If you do not check this box, the corresponding parameter setting does not take effect. If you set the parameters in the three configuration windows, the setting takes precedence in the following order:

1. Phone Configuration window
2. Common Phone Profile window
3. Enterprise Phone Configuration window

Corporate and Personal Directory setup

The Contact button on the Cisco Unified IP Phone gives users access to several directories. These directories can include:

Corporate Directory

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

Personal Directory

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

Corporate Directory setup

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 "Understanding Directory Numbers" in the *Cisco Unified Communications Manager System Guide*.

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

Personal Directory Setup

Personal Directory consists of the following features:

- Personal Address Book (PAB)
- Speed Dials
- Address Book Synchronization Tool (TABSynch)

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 Manager User Options web pages.
- From the Cisco Unified IP Phone: Choose Contacts to search the corporate directory or the user personal directory.
- From a Microsoft Windows application: Users can use the TABSynch tool to synchronize their PABs with Microsoft Windows Address Book (WAB). Customers who want to use the Microsoft Outlook Address Book (OAB) should begin by importing the data from the OAB into the WAB. TabSync can then be used to synchronize the WAB with Personal Directory. For instructions about TABSync, see

Obtain Cisco Unified IP Phone Address Book Synchronizer, on page 297 and Cisco Unified IP Phone Address Book Synchronizer Deployment, on page 297.

To ensure that Cisco IP Phone Address Book Synchronizer users access only their end-user data, activate the Cisco UXL Web Service in Cisco Unified Serviceability.

To configure Personal Directory from a web browser, users must access their User Options web pages. You must provide users with a URL and sign-in information.

Cisco IP Manager Assistant

Cisco IP Manager Assistant (IPMA) provides call routing and other call management features to help managers and assistants handle phone calls more effectively.

IPMA services must be configured in Cisco Unified Communications Manager before users can access them. For detailed information on configuring IPMA, see *Cisco Unified Communications Manager Administration Guide* and *Cisco Unified Communications Manager Features and Services Guide*.

IPMA has three key components:

Manager

A manager is the user whose incoming calls are intercepted by the call routing service.

Assistant

An assistant is the user who handles calls on behalf of a manager.

Assistant Console

The assistant console is a desktop application that can be used by assistants to perform tasks and manage most features.

IPMA supports two modes of operation: proxy line support and shared line support. Both modes support multiple calls per line for the manager. The IPMA service supports both proxy line and shared line support in a cluster.

In shared-line mode, the manager and assistant share a directory number and calls are handled on the shared line. Both the manager phone and the assistant phone ring when a call is received on the shared line. Shared-line mode does not support default assistant selection, assistant watch, call filtering or divert all calls.

In proxy-line mode, the assistant handles calls on behalf of a manager using a proxy number. Proxy-line mode supports all IPMA features.

IPMA softkey templates

IPMA features are accessed by softkeys and through Phone Services. The softkey template is configured in Cisco Unified Communications Manager. IPMA supports the following standard softkey templates:

Standard Manager

Supports manager for proxy mode.

Standard Shared Mode Manager

Supports manager for shared mode.

Standard Assistant

Supports assistant in proxy or in shared mode.

The following table describes the softkeys available in the softkey templates.

Table 24: IPMA softkeys

Softkey	Call State	Description
Redirect	Ringing, Connected, OnHold	Divert the selected call to a preconfigured target.
Intercept	All states	Divert a call from the assistant's phone to the manager's phone and autoanswer it.
Set Watch	All states	View the status of call being handled by an assistant.
TransVM	Ringing, Connected, OnHold	Redirect the selected call to the manager's voice mail.
Divert All	All states	Divert all calls that are routed to the manager to a preconfigured target.

Note Intercept, Set Watch, and Divert All should only be configured for a manager phone in proxy line mode.

Related Topics

Softkey template, on page 175

IPMA Proxy Line support

When you configure Cisco IPMA in proxy-line mode, the manager and assistant do not share a directory number. The assistant handles calls for a manager using a proxy number. The proxy number is not the directory number for the manager, but an alternate number chosen by the system and that an assistant uses to handle manager calls. In proxy-line mode, a manager and an assistant have access to all features that are available in IPMA, which include default assistant selection, assistant watch, call filtering, and divert all.

In order to access proxy-line support on user devices, you must first use Cisco Unified Communications Manager Administration to configure and start the Cisco IP Manager Assistant service.

For detailed information on configuring proxy-line support, see *Cisco Unified Communications Manager Administration Guide*, “Configure Cisco Unified Communications Manager Assistant with proxy line support” chapter.

IPMA Shared Line support

If you configure Cisco IPMA in shared-line mode, the manager and assistant share a directory number; for example, 1701. The assistant handles calls for a manager on the shared directory number. When a manager receives a call on directory number 1701, both the manager phone and the assistant phone rings.

Not all IPMA features are available in shared-line mode including default assistant selection, assistant watch, call filtering, and divert all calls. An assistant cannot see or access these features on the Assistant Console application. The assistant phone does not have the softkey for the divert all feature. The manager phone does not have the softkeys for assistant watch, call intercept, or divert all feature.

In order to access shared-line support on user devices, you must first use Cisco Unified Communications Manager Administration to configure and start the Cisco IP Manager Assistant service.

For detailed information on configuring shared-line support, see *Cisco Unified Communications Manager Administration Guide*, "Configure CUCM Assistant with shared line support" chapter.

Feature Buttons and Softkeys

The following table provides information about features that are available on softkeys, features that are available on dedicated feature buttons, and features that you need to configure as programmable feature buttons. An "X" in the table indicates that the feature is supported for the corresponding button type or softkey. Of the two button types and softkeys, only programmable feature buttons require configuration in Cisco Unified IP Phone administration.

For information about configuring programmable feature buttons, see the Phone Button Templates, on page 173. For information about configuring features that can appear as softkeys or programmable buttons, see Feature Control Policy, on page 178.

Table 25: Features and Corresponding Buttons and Softkeys

Feature name	Dedicated feature button	Programmable feature button	Softkey
Alert Calls		X	
All Calls		X	
Answer		X	
Call Back		X	X
Call Forward All		X	X
Call Park		X	X
Call Park Line Status		X	
Call Pickup (Pick Up)		X	X
Call Pickup Line Status		X	

Feature name	Dedicated feature button	Programmable feature button	Softkey
Conference	X		X (available while on a conference only)
Divert			X
Do Not Disturb		X	
Group Pickup (Group Pick Up)		X	X
Hide video Show video			X
Hold	X		
Hunt Groups		X	
Intercom		X	
Malicious Call Identification (MCID)		X	X
Meet Me		X	X
Mobile Connect (Mobility)		X	X
Mute	X		
Other Pickup		X	X
PLK Support for Queue Status			X
Privacy		X	
Queue Status		X	
Quality Reporting Tool (QRT)		X	X
Redial		X	X
Speed Dial		X	X
Speed Dial Line Status		X	X

Feature name	Dedicated feature button	Programmable feature button	Softkey
Support for Hold Button on USB Headsets			X
Transfer	X		X (available during a transfer only)

Phone Button Templates

Phone button templates let you assign speed dials and call-handling features to programmable buttons. Call-handling features that can be assigned to buttons include Answer, Mobility, and All Calls.

Ideally, you modify templates before you register phones on the network. In this way, you can access customized phone button template options from Cisco Unified Communications Manager during registration.

Note The default Cisco Unified IP Phone 9971 template that ships with the phone uses buttons 1 and 2 for lines.

Modify Phone Template

The Cisco Unified Communications Manager Device Settings page contains the phone template.

Procedure

Step 1 Choose **Device** > **Device Settings** > **Phone Button Template** in Cisco Unified Communications Manager Administration.

Step 2 To assign a phone button template to a phone, use the Phone Button Template field in the Cisco Unified Communications Manager Administration Phone Configuration window.
See the *Cisco Unified Communications Manager Administration Guide* and the *Cisco Unified Communications Manager System Guide* for more information.

Phone Button Template for All Calls

We recommend that you provision an **All Calls** button for users with multiple shared lines. When you configure an **All Calls** button on the phone, you enable the users to do the following:

- Press **All Calls** to display a consolidated list of current calls from all lines on the phone.
- Press **All Calls** under Call History to displays a list of all missed calls from all lines on the phone.

- Place a call on the user primary line when the user goes off-hook. All Calls automatically defaults to the user primary line for any outgoing call.

To add the **All Calls** button, modify the phone button template and then assign the template to the phone.

Phone Button Template for Personal Address Book or Speed Dials

You can modify a phone button template to associate a service URL with a programmable button. Doing so provides users with single-button access to the PAB and Speed Dials. Before you modify the phone button template, you must configure PAB or Speed Dials as an IP Phone service.

Set Up PAB or Speed Dial as IP Phone Service

To configure PAB or Speed Dial as an IP Phone service (if it is not already a service), follow these steps:

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Device** > **Device Settings** > **Phone Services**.
The Find and List IP Phone Services window displays.

Step 2 Click **Add New**.
The IP Phone Services Configuration window displays.

Step 3 Enter the following settings:

- Service Name and ASCII Service Name: Enter **Personal Address Book**.
- Service Description: Enter an optional description of the service.
- Service URL

  For PAB, enter the following URL:

  http://<Unified CM-server-name>**:8080/ccmpd/login.do?name=#DEVICENAME#&service=pab**

  For Fast Dial, enter the following URL:

  http://<Unified-CM-server-name>**:8080/ccmpd/login.do?name=#DEVICENAME#&service=fd**
- Secure Service URL

  For PAB, enter the following URL:

  https://<Unified CM-server-name>**:8443/ccmpd/login.do?name=#DEVICENAME#&service=pab**

  For Fast Dial, enter the following URL:

  https://<Unified-CM-server-name>**:8443/ccmpd/login.do?name=#DEVICENAME#&service=fd**
- Service Category: Select **XML Service**.
- Service Type: Select **Directories**.
- Enable: Select the check box.

  http://<IP_address> or *https://<IP_address>* (Depends on the protocol that the Cisco Unified IP Phone supports.)

Step 4 Select **Save**.
You can add, update, or delete service parameters as described in the "Cisco Unified IP Phone Services Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*.

Note If you change the service URL, remove an IP Phone service parameter, or change the name of a phone service parameter for a phone service to which users are subscribed, you must click **Update Subscriptions** to update all currently subscribed users with the changes; otherwise, users must resubscribe to the service to rebuild the correct URL.

Modify Phone Button Template for PAB or Fast Dial

For more information about IP Phone services, see "Cisco Unified IP Phone Services Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*. For more information about configuring line buttons, see "Cisco Unified IP Phone Configuration" chapter and "Configuring Speed-Dial Buttons" section in the *Cisco Unified Communications Manager Administration Guide*.

Procedure

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

Step 2 Click **Find**.

Step 3 Select the phone model.

Step 4 Select **Copy**, enter a name for the new template, and then select **Save**.
The Phone Button Template Configuration window opens.

Step 5 Identify the button that you would like to assign, and select **Service URL** from the Features drop-down list that associates with the line.

Step 6 Select **Save** to create a new phone button template that uses the service URL.

Step 7 Choose **Device** > **Phone** and open the Phone Configuration window for the phone.

Step 8 Select the new phone button template from the Phone Button Template drop-down list.

Step 9 Select **Save** to store the change and then select **Reset** to implement the change.
The phone user can now access the User Options web pages and associate the service with a button on the phone.

Softkey template

Using Cisco Unified Communications Manager Administration, you can associate a maximum of 18 softkeys with applications that are supported by the Cisco Unified IP Phone 8961, 9951 and 9971.
Cisco Unified Communications Manager supports the Standard User and Standard Feature softkey template.

An application that supports softkeys has one or more standard softkey templates associated with it. You modify a standard softkey template by copying it, renaming it, and then updating the new template. You can also modify a nonstandard softkey template.

The Softkey Control parameter shows if softkeys of a phone are controlled by the Feature Control Policy or the Softkey Template feature. The Softkey Control parameter is a required field.

The default is Feature Control Policy.

To configure softkey templates, select **Device** > **Device Settings** > **Softkey Template** from Cisco Unified Communications Manager Administration. To assign a softkey template to a phone, use the Softkey Template field in the Cisco Unified Communications Manager Administration Phone Configuration window.

For more information about configuring this feature, see the *Cisco Unified Communications Manager Administration Guide*, "Softkey Template Configuration" chapter, and the *Cisco Unified Communications Manager System Guide*, "Softkey Template" chapter.

The Cisco Unified IP Phones do not support all the softkeys that are configurable in Softkey Template Configuration on Cisco Unified Communications Manager Administration. Cisco Unified Communications Manager allows you to enable or disable some softkeys in the control policy configuration settings. The following table lists the features and the softkeys that can be configured on a softkey template, and identifies whether it is supported on the Cisco Unified IP Phones.

Note Cisco Unified Communications Manager allows you to configure any softkey in a softkey template, but unsupported softkeys do not display on the phone.

Table 26: Configurable softkeys

Feature	Configurable softkeys in the Softkey Template configuration	Supported as a softkey on Cisco Unified IP Phone 8961, 9951 and 9971	Notes
Answer	Answer (Answer)	Yes	—
Call Back	Call Back (CallBack)	Yes	—
Call Forward All	Forward All (cfwdAll)	Yes	Phone displays Forward All or Forward Off.
Call Park	Call Park (Park)	Yes	—
Call Pickup	Pick Up (Pickup)	Yes	—
cBarge	Conference Barge (cBarge)	Yes	Both Barge and cBarge are supported. But only one will be displayed on the phone.
Conference	Conference (Confrn)	Yes	Conference is a dedicated button.
Conference List	Conference List (ConfList)	Yes	Phone displays Show Detail.

Feature	Configurable softkeys in the Softkey Template configuration	Supported as a softkey on Cisco Unified IP Phone 8961, 9951 and 9971	Notes
Divert	Immediate Divert (iDivert)	Yes	Phone displays Divert.
Do Not Disturb	Toggle Do Not Disturb (DND)	Yes	Configure Do Not Disturb as a programmable line button or as a softkey.
End Call	End Call (EndCall)	Yes	—
Group Pickup	Group Pick UP (GPickUp)	Yes	—
Hold	Hold (Hold)	No	Hold is a dedicated button.
Hunt Group	HLog (HLog)	Yes	Configure Hunt Group as a programmable feature button.
Join	Join (Join)	No	—
Malicious Call Identification	Toggle Malicious Call Identification (MCID)	Yes	Configure Malicious Call Identification as a programmable feature button or as a softkey.
Meet Me	Meet Me (MeetMe)	Yes	—
Mobile Connect	Mobility (Mobility)	Yes	Configure Mobile Connect as a softkey.
New Call	New Call (NewCall)	Yes	—
Other Pickup	Other Pickup (oPickup)	Yes	—
PLK Support for Queue Statistics	Queue Status	No	—
Quality Reporting Tool	Quality Reporting Tool (QRT)	Yes	Configure Quality Reporting Tool as a programmable feature button or as a softkey.
Redial	Redial (Redial)	Yes	—
Remove Last Conference Participant	Remove Last Conference Participant (Remove)	No	—

Feature	Configurable softkeys in the Softkey Template configuration	Supported as a softkey on Cisco Unified IP Phone 8961, 9951 and 9971	Notes
Resume	Resume (Resume)	Yes	—
Select	Select (Select)	No	—
Speed Dial	Abbreviated Dial (AbbrDial)	Yes	Phone displays SpeedDial.
Transfer	Direct Transfer (DirTrfr)	Yes	Transfer is a dedicated button. Configure transfer (Direct Transfer policy) in the Product Specific Configuration Layout section in Phone Configuration.
Video Mode Command	Video Mode Command (VidMode)	No	—

Cisco IP Manager Assistant (IPMA) provides additional softkeys that can be controlled by the softkey template. For information on the IPMA softkeys, see Cisco IP Manager Assistant, on page 169

Feature Control Policy

You can limit the appearance of some telephony features on the Cisco Unified IP Phone 8961, 9951, and 9971 by enabling or disabling these features in the feature control policy configuration. When you disable a feature in the feature control policy configuration for a phone, you restrict user access to the feature and the softkeys for the feature do not display on the phone.

The Feature Control Policy also controls the display of the following features as either softkeys or programmable line keys:

- Malicious Caller ID
- Pick Up
- Group Pick Up
- Other Pick Up
- Meet Me
- Quality Reporting Tool
- Mobility

For more information, see the “Feature Control Policy” chapter in the *Cisco Unified Communications Manager Administration Guide*.

Create Feature Control Policy

To create a Feature Control Policy, follow these steps:

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Device** > **Device Settings** > **Feature Control Policy**.
The Find and List Feature Control Policy window displays.

Step 2 Click **Add New** to define a set of policies.

Step 3 Enter the following settings.

- Name: Enter a name for a new Feature Control Policy
- Description: Enter a description.
- Feature Control Section: Check the check box for the features for which you want to change the default setting. See Feature Control Policy Default Values, on page 179 for the list of features that can be configured and the default value.

Step 4 Click **Save**.

Step 5 Apply the policy to the phone by including it in the following windows:

- Enterprise Parameters Configuration: Applies to all phones in the system.
- Common Phone Profile Configuration: Applies to all phones in a group.
- Phone Configuration: Applies to an individual phone.

Feature Control Policy Default Values

The following table lists the features that a Feature Control Policy can control and their default values.

Table 27: Feature Control Policy Default Values

Feature	Default value
Forward All	Enabled
Park	Disabled
To Voicemail	Disabled
Conference List	Enabled
Speed Dial	Enabled

Feature	Default value
Call Back	Enabled
Redial	Enabled
Barge	Enabled
Malicious Caller ID	Disabled
Pick Up	Disabled
Group Pick Up	Disabled
Other Pick Up	Disabled
Meet Me	Disabled
Quality Reporting Tool	Disabled
Mobility	Disabled

Services Setup

You can give users access to Cisco Unified IP Phone Services on the Cisco Unified IP Phone 8961, 9951, and 9971. You can also assign a button to different phone services. These services comprise XML applications and Cisco-signed Java midlets that enable the display of interactive content with text and graphics on the phone. The Cisco Unified IP Phone manages each service as a separate application. Examples of services include local movie times, stock quotes, and weather reports.

Before a user can access any service:

- You must 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 Manager User Options application. 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.

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.

To set up these services, choose **Device** > **Device Settings** > **Phone Services** from Cisco Unified Communications Manager Administration. For more information, see the "Cisco Unified IP Phone Services Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide* and the "Cisco Unified IP Phone Services" chapter in the *Cisco Unified Communications Manager System Guide*.

After you configure these services, verify that your users can access the Cisco Unified Communications Manager User Options web-based application, from which they can select and subscribe to configured services.

See Phone Features User Subscription and Setup, on page 296 for a summary of the information that you must provide to end users.

Note To configure Cisco Extension Mobility services for users, see the "Cisco Extension Mobility" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

Add Users to Cisco Unified Communications Manager

Adding users to Cisco Unified Communications Manager allows you to display and maintain information about users and allows each user to perform these tasks:

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

You can add users to Cisco Unified Communications Manager by using one of these following methods:

- To add users individually, choose **User Management** > **End User** from Cisco Unified Communications Manager Administration.
  For more information, see the "End User Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*.
- 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 "Bulk Administration" chapter in the *Cisco Unified Communications Manager Administration Guide*.

User Options Web Pages Management

From the User Options web pages, users can customize and control several phone features and settings. For detailed information about the User Options web pages, see the user guide.

Set Up Access to User Options Web Pages

Before a user can access the User Options web pages, you must add the user to the standard Cisco Unified Communications Manager end user group and associate the appropriate phone with the user.

Make sure to provide end users with the following information about the User Options web pages:

- The URL for accessing the application. This URL is:
  http://<*server_name:portnumber*>/**ccmuser**/, 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 for accessing the application.

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

For more information, see:

- *Cisco Unified Communications Manager Administration Guide*, "User Group Configuration" chapter
- *Cisco Unified Communications Manager Administration Guide*, "End User Configuration" chapter
- *Cisco Unified Communications Manager Administrator Guide*, "Role Configuration" chapter

Add User to 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 Groups**. 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**.

Customize User Options Web Page Display

Most options that display on the User Options web pages appear by default. However, the system administrator must set the following options by using Enterprise Parameters Configuration settings in Cisco Unified Communications Manager Administration:

- Show Ring Settings
- Show Line Text Label Settings
- Show Call Forwarding

Note The settings apply to all User Options web pages at your site.

To specify the options that appear on the User Options web pages, perform these steps:

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **System** > **Enterprise Parameters**.
The Enterprise Parameters Configuration window appears.

Step 2 In the CCMUser Parameters area, specify whether a parameter displays on the User Options web pages by choosing one of these values from the Parameter Value drop-down list for the parameter:

- **True**: Option displays on the User Options web pages (default except for Show Ring Settings, Show Line Text Label, and Show Call Forwarding).
- **False**: Option does not display on the User Options web pages.
- **Show All Settings**: All Call Forward settings display on the User Options web pages (default).
- **Hide All Settings**: No Call Forward settings display on the User Options web pages.
- **Show Only Call Forward All**: Only Call Forward All calls displays on the User Options web pages.

Feature Setup

This section contains additional procedures for setting up some of the phone features.

Set Up Automatic Port Synchronization

To configure the parameter in the Cisco Unified Communications Manager Administration application, choose **Device** > **Phone**, select the appropriate IP phones, and scroll to the Product Specific Configuration Layout pane.

To configure the setting on multiple phones simultaneously, enable Automatic Port Synchronization in the Enterprise Phone Configuration window (**System** > **Enterprise Phone Configuration**).

Set up Bluetooth profiles

For more information on Bluetooth profiles, see the *Cisco Unified Communications Manager Administration Guide*.

Procedure

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

Step 2 Find your phone from the list of phones that display in Cisco Unified Communications Manager.

Step 3 Click on the **Device Name** of the phone.
The Phone Configuration window appears.

Step 4 Go to the Product Specific Configuration Layout area and from the Bluetooth Profiles drop-down list, choose the applicable profile.
The Handsfree profile is selected by default.

Step 5 Check the Override Common Settings check box for any setting in the Product Specific Configuration area that you wish to update.

- If you do not check this check box, the corresponding parameter setting does not take effect.
- Parameters that you set in the Product Specific Configuration area may also appear in the Device Configuration window for various devices and in the Enterprise Phone Configuration window.

If you also set these same parameters in these other windows, the setting that takes precedence is determined in the following order:

1 Device Configuration window settings (highest precedence)

2 Common Phone Profile Configuration window settings

3 Enterprise Phone Configuration window settings (lowest precedence)

Call Forward Notification Setup

You set up the information that the user sees from Cisco Unified Communications Manager Administration in the Device Configuration window (**Device** > **Phone**). The following table describes the Call Forward Notification fields.

Table 28: 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.
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.

Client Matter Codes Setup

To force users to enter a Client Matter Code (CMC) when placing a call, configure the fields in the Client Matter Code Configuration window (**Call Routing** > **Client Matter Codes**). The following table describes the Client Matter Code field.

Table 29: CMC Field

Field	Description
Require Client Matter Code	This check box controls whether the system prompts the user for a CMC upon placing a call.

For more information, see the "Route Pattern Configuration" chapter of the *Cisco Unified Communications Manager Administration Guide*.

Enable Line Status for Call Lists

To enable the Line Status for Call Lists perform the following procedure:

Procedure

Step 1 Go to Cisco Unified CM Administration and choose **System** > **Enterprise Parameters**.
The Enterprise Parameters Configuration window appears.

Step 2 From the Line Status for Call Lists drop-down list box, choose the applicable profile.
The Disabled option is selected by default.

Parameters that you set in the Product Specific Configuration area may also appear in the Device Configuration window for various devices and in the Enterprise Phone Configuration window.

If you set these same parameters in these other windows as well, the setting that takes precedence is determined in the following order:

1. Device Configuration window settings
2. Common Phone Profile window settings
3. Enterprise Phone Configuration window settings

Set Up Dual Bank Information

To set up Dual Bank Information, follow these steps:

Procedure

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

Step 2 Check the load information in the Inactive Load Information field.

Step 3 Choose **Bulk Administration** > **Import/Export** > **Export** > **Device Defaults**, and schedule an export job.

Step 4 Download the exported tar file and untar it.

Step 5 Check the file format in the exported CSV file and verify that the CSV file has an Inactive Load Information column with the correct value.

Note The CSV file value must match the Device Default value in the Cisco Unified Communications Manager Administration window.

Forced Authorization Codes Setup

To force users to enter a Forced Authorization Code (FAC) when placing a call, configure the fields in the Forced Authorization Code Configuration window (**Call Routing** > **Forced Authorization Code**). The following table describes the Forced Authorization Code fields.

Table 30: FAC Field

Field	Description
Require Forced Authorization Code	Select the check box to require a user to enter an FAC.
Authorization Level	The code that the user must enter to be authorized to place the call.

For more information, see the "Route pattern setup" chapter of the *Cisco Unified Communications Manager Administration Guide*.

Incoming Call Toast Timer Setup

You can set the time that the Incoming Call Toast (incoming call notification window) displays on the user phone. You set up the feature from one of the following Cisco Unified Communications Manager windows:

- Enterprise Phone Configuration (**System** > **Enterprise Phone**)
- Common Phone Profile Configuration (**Device** > **Device Settings** > **Common Phone Profile**)
- Phone Configuration (**Device** > **Phone**)

The following table describes the Incoming Call Toast Timer.

Table 31: Incoming Call Toast Timer Field

Field	Description
Incoming Call Toast Timer	Gives the time, in seconds, that the toast displays. The time includes the fade-in and fade-out times for the window. The possible values are 3, 4, 5, 6, 7, 8, 9, 10, 15, 30, and 60. The default is 5.

Set Up Peer Firmware Sharing

When enabled, the feature allows the phone to discover like phones on the subnet that are requesting the files that make the firmware image, and to automatically assemble transfer hierarchies on a per-file basis. The individual files making up the firmware image are retrieved from the TFTP server by only the root phone in

the hierarchy, and the files are then rapidly transferred down the transfer hierarchy to the other phones on the subnet that are using TCP connections.

This menu option indicates whether the phone supports peer firmware sharing. Settings include:

- Enabled, which is the default value.
- Disabled

Note Phone firmware release 9.1(1) supports HTTP and TFTP firmware download methods.

To set up Peer Firmware Sharing, follow these steps:

Procedure

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

Step 2 Find your phone from the list of phones that associate with the Cisco Unified Communications Manager.

Step 3 Click on the Device Name of the phone.
The Phone Configuration window appears.

Step 4 Go to Product Specific Configuration Layout area and select **Enable** from the Peer Firmware Sharing drop-down list.
The Peer Firmware Sharing is enabled by default.

Step 5 Check the Override Common Settings check box for any setting in the Product Specific Configuration area that you wish to update.

- If you do not check this check box, the corresponding parameter setting does not take effect.
- Parameters that you set in the Product Specific Configuration area may also appear in the Phone Configuration window for various devices and in the Enterprise Phone Configuration window.

If you set these same parameters in these other windows too, the setting that takes precedence is determined in the following order:

1. Device Configuration window settings (highest precedence)
2. Common Phone Profile window settings
3. Enterprise Phone Configuration window settings (lowest precedence)

Remote Port Configuration Setup

To configure the Switch Remote Port Configuration parameter or the PC Remote Port Configuration parameter, you have two options in the Cisco Unified Communications Manager Administration application:

- To configure the parameter for individual phones, choose **Device** > **Phone**, select the appropriate IP Phones, and scroll to the Product Specific Configuration Layout area (Switch Port Remote Configuration or PC Port Remote Configuration).

- To configure the setting on multiple phones simultaneously, configure the Remote Port Configuration in the Enterprise Phone Configuration window (**System** > **Enterprise Phone Configuration**).

Enable Device Invoked Recording

Configure the Device Invoked Recording feature from Cisco Unified Communications Manager Administration. For more information and detailed instructions, see the "Monitoring and Recording" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

Procedure

Step 1 Set the IP phone Built In Bridge to **On**.

Step 2 Set Recording Option to **Selective Call Recording Enabled**.

Step 3 Select the appropriate Recording Profile.

Enable Call History for Shared Line

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

Procedure

Step 1 Go to Cisco Unified CM Administration and choose **Device** > **Phone**.

Step 2 Find your phone from the list of phones associated with the Cisco Unified CM.

Step 3 Click on the Device Name of the phone.
The Phone Configuration window appears.

Step 4 Go to Product Specific Configuration Layout area and from the Logging Display drop-down list box, choose the applicable profile.
The Disabled option is selected by default.

Parameters that you set in the Product Specific Configuration area may also appear in the Device Configuration window for various devices and in the Enterprise Phone Configuration window.

If you set these same parameters in these other windows as well, the setting that takes precedence is determined in the following order:

1 Device Configuration window settings

2 Common Phone Profile window settings

3 Enterprise Phone Configuration window settings

Pause in Speed Dial

With this feature, users can set up the speed dial feature to reach destinations that require Forced Authorization Code (FAC) or Client Matter Code (CMC), dialing pauses, and additional digits (such as a user extension, a meeting access code, or a voicemail password) without manual intervention. When the user presses the speed dial, the phone establishes the call to the specified DN and sends the specified FAC, CMC, and DTMF digits to the destination with dialing pauses inserted.

To include dialing pauses in the speed dial, the user must specify a comma (,) in the speed dial string. Each comma indicates a pause of 2 seconds. The comma also acts as a delimiter between destination digits, the FAC, CMC, and additional DTMF digits. The comma as delimiter is useful in the following cases:

- Differentiates overlapping dial patterns (for example 9.xxx from 9.xxxxx)
- Identifies the destination number when using variable-length dial patterns (for example 9.!)
- Differentiates overlapping FAC or CMC (for example, 8787 from 87879)

Note Be aware of the following requirements when you include FAC and CMC in the speed dial string:

- FAC must always precede CMC in the speed dial string.
- A speed dial label is required for speed dials containing FAC and DTMF digits.
- Only one comma is allowed between FAC and CMC digits in the string.

For any additional DTMF digits specified after the FAC and CMC, the phone dials these additional digits (with pauses) after the call is connected.

Non-Comma Delimited Speed Dial Strings

You can configure speed dial strings without using a comma as a delimiter. In this case, you can enter all the digits (DN, FAC, CMC, and DTMF) as one continuous string. This continuous string can be used for calls made using fixed-length route patterns. However, the configured string may not function with overlapping route patterns or overlapping FAC or CMC. Cisco recommends that you use comma-delimited speed dial strings for best results.

Note Non-comma-delimited strings work only when FAC or CMC is enabled on the route pattern. This configuration cannot be used only with DTMF digits.

InterDigit Interval

The InterDigit Interval allows the administrator to configure the interval between sending digits in the string. The default InterDigit Interval is 60 ms. The range is 50 ms to 500 ms.

Note that this value does not alter the pause value (2 seconds) indicated by the comma.

Errors with Incorrect CMC or FAC

If the user enters an incorrect FAC or CMC in a comma-delimited speed dial string and then presses the speed dial label, the phone displays the following error message:

```
Error: Invalid Code in SpeedDial
```

If the user does not use commas as delimiters, and there is an error in the FAC or CMC, the phone prompts the user to enter the required codes manually.

SRST and CME

When a comma-delimited string is used on a phone operating in SRST or CME mode, the phone sends the digits up to the first comma, and then the user manually adds the required codes.

If a non-comma-delimited string is used with SRST or CME, the phone sends the full string, and the call may fail.

Assured Services for SIP Lines

Depending on how you have configured your phone system, users may be able to make priority calls using the Assured Services for SIP Lines (AS-SIP) feature.

With this feature, routine calls are placed normally. However, during an emergency, users can select a priority level that helps ensure the delivery of critical calls. Depending upon how the user's telephone is configured, they may be required to enter login information also.

When the user receives a priority call, a precedence level icon displays next to the caller's name on their phone.

AS-SIP Setup in SIP Profile

The SIP profile contains an 'Is Assured SIP Service Enabled' check box. This check box should be checked for third-party AS-SIP endpoints as well as for AS-SIP trunks to ensure proper Assured Service behavior.

This setting provides specific Assured Service behavior that affects services such as Conference factory and SRTP.

Third-Party AS-SIP Device Setup

The phone Add list displays the third-party AS-SIP phone as an available choice.

The device configuration fields are the same as those for Cisco phones.

Resource Priority Namespace Setup

The Resource Priority namespace for an AS-SIP phone is configured in the phone section of the SIP Profile.

An AS-SIP phone is associated with a single Resource Priority namespace.

If <*None*> is left as the namespace in the SIP profile then the default namespace is used.

MLPP Device Setup

The following MLPP configuration fields are located on the device page:

- MLPP Domain
- MLPP Indication
- MLLP Preemption

The MLPP Preemption value is only configurable for Cisco AS-SIP devices. For third party AS-SIP devices, the determination about whether a call can be preempted is left to the device.

MLPP Precedence Domain Setup

MLPP domain is configured at the device level.

The range of values is 000000 – FFFFFF.

This value is used during preemption decisions. Only calls within the same precedence domain can be preempted.

MLPP Indication Setup

MLPP can be enabled for the device at 3 different levels – device, common configuration and the enterprise parameter level.

Set the MLPP Indication to **On** to enable MLPP regardless of the enterprise or common config settings.

Set the MLPP Indication to **Default** to cause MLPP to be enabled for the device if it is enabled at the common device config or enterprise parameter levels.

When MLPP Indication is set to **Off**, MLPP is disabled for the device regardless of the common device or enterprise parameter configuration.

MLPP Preemption Setup

MLPP preemption determines whether preemption for reuse can be performed on the device. This type of preemption is used to remove an existing call and offer a higher precedence call to the user of the device.

When set to **Disabled**, only preemption 'not for reuse' can be performed on the device. This type of preemption occurs when the user of the device is not the called party but is either in a call with the called party or is using a network resource that is preempted; for example, a trunk channel or reserved bandwidth allocation.

When set to **Forceful**, preempt for reuse is enabled and existing calls may be preempted to offer a higher precedence call to the user of the device.

When set to **Default**, the setting from the common configuration or enterprise level is used.

MLPP Authorization Setup for SIP Profile

Enable MLPP Authorization for a device by checking the MLPP User Authorization check box in the phone section of the SIP Profile used for the device.

When the check box is enabled, the system challenges the Cisco or third-party AS-SIP phone for the user's credentials when a precedence call is initiated from the device.

MLPP Authorization Setup for End User

Configure MLPP Authorization for a user on the End User administration page.

The MLPP User Identification number must be composed of 6 – 20 numeric characters.

The MLPP Password must be composed of 4 – 20 numeric (0-9) characters

The Precedence Authorization level can be set to any standard precedence level from Routine to Executive Override

MLPP DSCP Setup for End User

The DSCP values for video streams can be configured for each precedence level in the QOS section of the Service Parameters. All DSCP values include the decimal value in the setting.

Enable Video On/Off Setting

The Enable Video On/Off setting improves the video conference call flow by removing the black box that is displayed when one party has the Auto Transmit setting on their phone set to Off.

This setting works in conjunction with **Auto Transmit**. If the Enable Video feature is set to **Off**, it overrides the Auto Transmit setting and you can send audio calls. But if Enable Video is set to **On** and Auto Transmit is set to **Off**, the video stream is blocked and the user sends a black box to the other party. For this feature to function, Cisco recommends Auto Transmit remains **On**.

The Enable Video On/Off setting functions like Video Capability: Enable/Disable on Cisco Unified Communications Manager (Unified CM). However, the server settings override the phone settings so if video is disabled on the Unified CM, this feature is not available on the phone and all calls are audio only.

Dial Tone from Release Button Setup

You can provide users with one-button access to the dial tone and the New Call window from an active call.

You enable this option from one of the following Cisco Unified Communications Manager windows:

- **System** > **Enterprise Phone Configuration**
- **Device** > **Device Settings** > **Common Phone Profile**
- **Device** > **Phone** > **Phone Configuration**

The following table describes the field for the Dial Tone from Release button feature.

Field	Description
Provide Dial Tone from Release Key	Identifies if pressing the Release key causes the user to hear dial tone (Enabled) or not (Disabled). The possible values are Disabled or Enabled. The default is Disabled

Set Headset Sidetone Controls

Procedure

Step 1 Go to Cisco Unified CM Administration and choose **Device** > **Phone**.

Step 2 Find your phone from the list of phones associated with the Cisco Unified CM.

Step 3 Click on the Device Name of the phone.
The Phone Configuration window appears.

Step 4 Go to **Product Specific Configuration Layout** area and from the Wideband Headset UI Control drop-down list box, choose the applicable profile.

Step 5 The Off option is selected by default (should be enabled only if the user headset supports wideband).

Step 6 Parameters that you set in the Product Specific Configuration area may also appear in the Device Configuration window for various devices and in the Enterprise Phone Configuration window.
If you set these same parameters in these other windows as well, the setting that takes precedence is determined in the following order:

1. Device Configuration window settings
2. Common Phone Profile window settings
3. Enterprise Phone Configuration window settings

Park Monitoring

Park monitoring is supported only when a Cisco Unified IP Phone 8961, 9951, or 9971 parks a call. Park monitoring then monitors the status of a parked call. The park monitoring call bubble is not cleared until the parked call gets retrieved or is abandoned by the parkee. This parked call can be retrieved by using the same call bubble on the parker's phone.

Park Monitoring Service Parameters

Cisco Unified Communications Manager Administration provides three clusterwide service timer parameters for park monitoring: Park Monitoring Reversion Timer, Park Monitoring Periodic Reversion Timer, and Park Monitoring Forward No Retrieve Timer. Each service parameter includes a default and requires no special

configuration. These timer parameters are for park monitoring only; the Call Park Display Timer and Call Park Reversion Timer are not used for park monitoring. See the following table for descriptions of these parameters.

Table 32: Service Parameters for Park Monitoring

Field	Description
Park Monitoring Reversion Timer	Default is 60 seconds. This parameter determines the number of seconds that Cisco Unified Communications Manager waits before prompting the user to retrieve a call that the user parked. This timer starts when the user presses Park on the phone, and a reminder is issued when the timer expires. You can override the value that this service parameter specifies on a per-line basis in the Park Monitoring section of the Directory Number Configuration window (in Cisco Unified Communications Manager Administration, choose **Call Routing** > **Directory Number**). Specify a value of 0 to immediately utilize the periodic reversion interval that the Park Monitoring Periodic Reversion Timer service parameter specifies. (See the description that follows.) For example, if this parameter is set to zero and the Park Monitoring Periodic Reversion Timer is set to 15, the user is immediately prompted about the parked call and every 15 seconds thereafter until the Park Monitoring Forward No Retrieve Timer (see the description that follows) expires.
Park Monitoring Periodic Reversion Timer	Default is 30 seconds. This parameter determines the interval (in seconds) that Cisco Unified Communications Manager waits before prompting the user again that a call is parked. To connect to the parked call, the user can simply go off-hook during one of these prompts. Cisco Unified Communications Manager continues to prompt the user about the parked call as long as the call remains parked and until the time that the Park Monitoring Forward No Retrieve Timer (see the description that follows) specifies expires. Specify a value of 0 to disable periodic prompts about the parked call.
Park Monitoring Forward No Retrieve Timer	Default is 300 seconds. This parameter determines the number of seconds that park reminder notifications occur before the parked call forwards to the Park Monitoring Forward No Retrieve destination that is specified in the parker Directory Number Configuration window. (If no forward destination is provided in Cisco Unified Communications Manager Administration, the call returns to the line that parked the call.) This parameter starts when the time that the Park Monitoring Reversion Timer service parameter specifies expires. When the Park Monitoring Forward No Retrieve Timer expires, the call is removed from park and forwards to the specified destination or returns to the parker line.

Set Timers

Configure the timers in the Cisco Unified Communications Manager Service Parameters page.

Procedure

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

Step 2 Update the Park Monitoring Reversion Timer, Park Monitoring Periodic Reversion Timer, and Park Monitoring Forward No Retrieve Timer fields in the **Clusterwide Parameters (Feature-General)** pane.

Park Monitoring Parameters in Directory Number Configuration Window

The Directory Number Configuration window (in Cisco Unified Communications Manager Administration, choose **Call Routing** > **Directory Number**) contains a Park Monitoring area where you can configure the three parameters that the following table describes.

Table 33: Park Monitoring Parameters in Directory Number Configuration Window

Field	Description
Park Monitoring Forward No Retrieve Destination External	When the parkee is an external party, the call forwards to the specified destination in the parker Park Monitoring Forward No Retrieve Destination External parameter. If the Forward No Retrieve Destination External field value is empty, the parkee is redirected to the parker line.
Park Monitoring Forward No Retrieve Destination Internal	When the parkee is an internal party, the call forwards to the specified destination in the parker's Park Monitoring Forward No Retrieve Destination Internal parameter. If the Forward No Retrieve Destination Internal is empty, the parkee is redirected to the parker line.
Park Monitoring Reversion Timer	This parameter determines the number of seconds that Cisco Unified Communications Manager waits before prompting the user to retrieve a call that the user parked. This timer starts when the user presses Park on the phone, and a reminder is issued when the timer expires. Default: 60 seconds **Note** If you configure a nonzero value, this value overrides the value of this parameter set in the Service Parameters window. However, if you configure a value of 0 here, then the value in the Service Parameters window is used.

Park Monitoring Parameter in Hunt Pilot Configuration Window

When a call that was routed via the hunt list is parked, the Hunt Pilot Park Monitoring Forward No Retrieve Destination parameter value is used (unless it is blank) when the Park Monitoring Forward No Retrieve Timer expires. Configure this value in the Hunt Pilot Configuration window (in Cisco Unified Communications Manager Administration, choose **Call Routing** > **Route/Hunt** > **Hunt Pilot**).

If the Hunt Pilot Park Monitoring Forward No Retrieve Destination parameter value is blank, the call forwards to the destination that is configured in the Directory Number Configuration window when the Park Monitoring Forward No Retrieve Timer expires.

Actionable Incoming Call Alert Configuration

When this feature is enabled, an actionable alert displays when there is an incoming call. The alert will replace the traditional incoming call pop-up notification, and the user must respond to the alert.

The Actionable Incoming Call Alert configuration parameter controls the behavior of this feature. There are three possible settings for this new parameter:

Table 34: Actionable Incoming Call Alert Parameters

Parameter	Description
Disabled	The default state of the feature. The actionable incoming call alert is disabled. The traditional incoming call pop-up alert displays.
Show for all Incoming Call	The actionable incoming call alert displays for all calls regardless of visibility.
Show for Invisible Incoming Call	The actionable incoming call alert displays for calls not shown on the phone. This parameter behaves similarly to the incoming call alert pop-up notification.

Note If both the Custom Line Filters and the Actionable Incoming Call Alert features are enabled, actionable call alerts apply only to the lines that are covered by filters.

Enable Actionable Incoming Call Alert

Procedure

Step 1 Go to Cisco Unified Communications Manager Administration and choose one of the following:

- **System** > **Enterprise Phone Configuration**
- **Device** > **Device Settings** > **Common Phone Profile**
- **Device** > **Phone**

Step 2 Locate the Actionable Incoming Call Alert field and set the field to the appropriate setting.
The field is set to Disabled by default.

If you also configure this field in the other windows, the setting precedence is:

1 Device Configuration window settings
2 Common Phone Profile window settings
3 Enterprise Phone Configuration window settings

Enable Call History Display Enhancement

Procedure

Step 1 Go to Cisco Unified Communications Manager Administration and choose **Device** > **Phone**.

Step 2 Find your phone from the list of phones associated with the Cisco Unified Communications Manager.

Step 3 Click on the Device Name of the phone.
The Phone Configuration window appears.

Step 4 Go to Product Specific Configuration Layout area and from the Logging Display drop-down list box, choose **Enable**.
The Disabled option is selected by default.

Parameters that you set in the Product Specific Configuration area may also appear in the Device Configuration window for various devices and in the Enterprise Phone Configuration window.

If you set these same parameters in these other windows as well, the setting that takes precedence is determined in the following order:

1 Device Configuration window settings
2 Common Phone Profile window settings
3 Enterprise Phone Configuration window settings

Custom Line Filter Setup

This feature provides configurable options that help reduce alert activity by filtering it to high-priority lines as desired. Only you can configure or edit the default phone filter.

When the default line filter is configured, a filter named Daily schedule is available to users under the Call notifications options in the **Settings** > **Preferences** menu of the phone. This daily schedule filter is in addition to the preset All Calls filter.

If the default line filter is not configured, the phone checks all provisioned lines. If configured, the phone checks the lines set on Cisco Unified Communications Manager if the user selects Default filter as the active filter, or if there are no custom filters.

Table 35: Custom Line Filter Fields

Field	Description
Default line filter	A comma-separated list of phone device names to be included in the default filter. By default, the list is blank, and all provisioned lines are checked.

Custom line filters are set in the following window:

- **Device** > **Phone**

Set Up Default Line Filter

Procedure

Step 1 Go to Cisco Unified Communications Manager Administration and choose:

- **Device** > **Phone**

Step 2 Locate the Default Line Filter field and enter the line DN. Separate device name entries with a comma. The specified line is added to the default filter.

Set up Separate Audio and Video Mute

You can control the ability of your users to mute the audio on a call.

Procedure

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

Step 2 To enable the feature, set the Separate Audio and Video parameter to **Enabled**.

Step 3 Select **Save**.

Enable Softkey Policy Control

Softkey Policy Control enables you to configure the following features as softkeys or programmable feature buttons:

- Malicious Caller ID
- Pick Up

- Group Pick Up
- Other Pick Up
- Meet Me
- Quality Reporting Tool
- Mobility

For more information, see:

- *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phone" chapter
- *Cisco Unified Communications Manager Administration Guide*, "Phone Button Template Configuration" chapter

Procedure

Step 1 In the Cisco Unified Communications Manager Administration, navigate to **Device** > **Phone**.

Step 2 Find the phone that you need to set up and click the hyperlink for the phone.

Step 3 Set the Softkey Control field to **Softkey Template**.
The default value is Feature Control Policy.

Step 4 Select **Save**.

Set up RTP/sRTP port range

You configure the Real-Time Transport Protocol (RTP) and secure Real-Time Transport Protocol (sRTP) port values in the SIP profile. RTP and sRTP port values range from 2048 to 65535, with a default range of 16384 to 32764. Some port values within the RTP and sRTP port range are designated for other phone services. You cannot configure these ports for RTP and sRTP.

For more information, see the "SIP profile setup" chapter, in the *Cisco Unified Communications Manager Administration Guide*.

Procedure

Step 1 Select **Device** > **Device Settings** > **SIP Profile**

Step 2 Choose the search criteria to use and click **Find**.

Step 3 Select the profile to modify.

Step 4 Set the Start Media Port and Stop Media Port to contain the start and end of the port range.
The following list identifies the UDP ports that are used for other phone services and thus not available for RTP and sRTP use:

port 4051

used for the Peer Firmware Sharing (PFS) feature

port 5060

used for SIP over UDP transport

port range 49152 to 53247

used for local ephemeral ports

port range 53248 to 65535

used for the VxC single tunnel VPN feature

Step 5 Click **Save**.

Step 6 Click **Apply Config**.

TLS Session Resumption Timer

TLS Session resumption enables a TLS session to resume without repeating the entire TLS authentication process. It can significantly reduce the time taken for TLS connection to exchange data.

Although Cisco Unified IP Phones 8961, 9951, and 9971 support TLS sessions, all TLS sessions do not support TLS resumption. The following list describes the different sessions and TLS resumption support:

- TLS session for SIP signaling: supports resumption
- HTTPs client: supports resumption
- CAPF: supports resumption
- TVS: supports resumption
- EAP-TLS: does not support resumption
- EAP-FAST: does not support resumption
- VPN client: does not support resumption

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

Set up audio and video port range

Audio and video traffic can be sent to different RTP port ranges in order to improve Quality of Service (QoS).

The following fields control the port ranges in the Cisco Unified Communications Manager Administration:

- Audio ports
  - Start Media Port (default: 16384)
  - Stop Media Port (default:32766)
- Video ports

- Start Video RTP Port
- Stop Video RTP Port

The following rules apply when configuring the video port fields:

After the Start Video RTP Port and Stop Video RTP Port are configured, the phone uses ports within the video port range for video traffic. The audio traffic uses the media ports.

If the audio and video port ranges overlap, the overlapped ports carry both audio and video traffic. If the video port range is not configured correctly, the phone uses the configured audio ports for both audio and video traffic.

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

Procedure

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

Step 2 Set the Start Media Port and Stop Media Port fields for the audio port range.
Audio ports can be configured to use ports 16384 to 32766.

Step 3 Select **Save**.

Step 4 Select one of the following windows:

- **System** > **Enterprise Phone Configuration**
- **Device** > **Device Settings** > **Common Phone Profile**
- **Device** > **Phone** > **Phone Configuration**

Step 5 Set the Start Video RTP Port and Stop Video RTP Port fields for the range of ports required.
The following rules apply when configuring the video port fields:

- Each field must contain a number between 2048 and 65535.
- The value in the Stop Video RTP Port field must be larger than the value in the Start Video RTP Port field.
- The difference between the Start Video RTP Port field and the Stop Video RTP Port field must be at least 16.

Step 6 Select **Save**.

Cisco VXC VPN

The Cisco VXC VPN feature provides integrated VPN functionality for Cisco Virtualization Experience Clients (Cisco VXC) 2111 and 2112. The feature enables VPN tunneling for the Cisco VXC 2111 and Cisco VXC 2112 clients when they attach to a Cisco Unified IP Phone 8961, 9951, or 9971.

You can set up the Cisco VXC VPN and the phone VPN to use the same tunnel or separate tunnels in the following configurations:

- One tunnel for both Cisco VXC VPN traffic and phone VPN traffic
- Two tunnels that use the same access credentials (one for Cisco VXC VPN traffic and another for phone VPN traffic)
- Two tunnels that use different access credentials (one for Cisco VXC VPN traffic and another for phone VPN traffic). This configuration is only supported when a one-time password is applied.

You can configure the feature to prompt the user only once for access credentials (in the Phone VPN Sign In window), or once each for the phone VPN (in the Phone VPN Sign In window) and for the Cisco VXC VPN (in the VXC VPN Sign In window).

Cisco VXC VPN Setup

To set up the Cisco VXC VPN feature, you must first set up the VPN feature for the attached IP phone in Cisco Unified Communications Manager Administration. Use the submenus under the **Advanced Features** > **VPN** menu path.

To enable the Cisco VXC VPN feature after you enable the IP Phone VPN, you must populate the Enable VXC VPN for MAC field by using any of the following configuration windows:

- Phone Configuration window (**Device** > **Phone**)
- Common Phone Profile window (**Device** > **Device Settings** > **Common Phone Profile**)
- Enterprise Phone Configuration window (**System** > **Enterprise Phone Configuration**)

Note The Cisco VXC clients require no configuration to support the VPN. All VPN configuration is performed for the phone only.

The following table describes the Cisco VXC VPN fields.

Table 36: Cisco VXC VPN fields

Parameter name	Parameter description
Enable VXC VPN for MAC	This field enables or disables the Cisco VXC VPN feature. When you populate this field, the phone allows traffic from the device with the specified MAC address and that connects to the phone PC Port to access the tunnel. • When this field is blank, the phone does not establish a Cisco VXC VPN tunnel. • When this field specifies one broadcast MAC address (FFFFFFFFFFFF), the phone establishes the Cisco VXC VPN tunnel and allows any connected Cisco VXC 2111/2112 device to access the tunnel. • When this field specifies one nonbroadcast MAC address, the phone establishes the Cisco VXC VPN tunnel and allows only the Cisco VXC device with the specified MAC address to access the tunnel. By default, this field is blank.

Parameter name	Parameter description
VXC VPN Option	This field indicates the type of VXC VPN support. • Dual Tunnel: The phone establishes two VPN tunnels, one for the phone and another for the Cisco VXC device. To ensure the highest quality of service for the phone voice and video services, Cisco recommends the Dual Tunnel setting, which is the default setting. With two VPN tunnels, the host Cisco Unified IP Phone can provide prioritization of CPU and memory resources to the data that associates with the phone voice and with video functions over the data that associates with the Cisco VXC VPN tunnel. This approach requires two manual login entries, depending on security parameters: one for the phone VPN and another for the Cisco VXC VPN. The two-tunnel approach also requires two VPN concentrator ports and two IP addresses. • Single Tunnel: The phone establishes only one VPN tunnel for the phone and the Cisco VXC device to share. For customers who are willing to trade off potential voice and video quality for a simplified operating model, the single VPN tunnel option is available. All data travels over a single VPN tunnel by sharing the available phone processor and memory resources across the voice, video, and Cisco VXC services. The IP phone does not prioritize data handing of one service over another. As a result, possible performance degradation of the IP phone voice and video media handling and UI functions may occur due to IP phone CPU loading. Default: Dual Tunnel

Parameter name	Parameter description
VXC challenge	This field indicates whether or not to challenge the user for a password for the Cisco VXC VPN. **1** Challenge: The phone challenges the user for a password to enable the Cisco VXC VPN. **2** No Challenge: The phone does not challenge the user for a password for the Cisco VXC VPN. Default: Challenge **Note** If the phone uses only a certificate for authentication, the Sign In windows do not display.
VXC-M Servers	This field indicates the Cisco VXC Manager Server IP address list, where each entry is separated by commas. Maximum length: 255 (character length) Default: blank **Note** VXC-M Servers is an IP address list which includes VXC-M servers and repository servers (if present). The phone considers the first IP address in this string as the VXC-M server and offers this information to VXC devices. Therefore, after you configure VXC-M Servers, make sure that the IP addresses of any VXC-M servers are placed in front of the IP addresses of the repository servers.

The following table describes how the VXC VPN Option and Challenge field settings alter the operation of the Cisco VXC VPN feature.

Table 37: Cisco VXC VPN operation as determined by VXC VPN Option and Challenge settings

VXC VPN Option setting	VXC Challenge setting	Result after enabling the VXC VPN feature (with Cisco VXC connected to the phone)
Dual Tunnel (default)	Challenge (default)	The phone displays the VXC VPN Sign In window to prompt the user to enter a password. If one-time password is configured on the VPN concentrator (that is, a new password is always required to reauthenticate the tunnel), the user must enter a password for the Cisco VXC VPN that differs from the password that was used for the phone VPN tunnel.
Dual Tunnel (default)	No Challenge	The phone attempts to reuse the phone VPN credentials for the Cisco VXC VPN tunnel. Note that if the VPN concentrator is configured for one-time passwords, the attempt fails, and the phone displays the VXC VPN Sign In window for the user to enter a different password from the phone VPN password.
Single Tunnel	Challenge	The phone disconnects the phone VPN tunnel, and then displays the Phone VPN Sign In window to prompt the user to enter a password and reestablish the phone VPN tunnel. If the user is on an active call, the phone waits until the call ends before tearing down the tunnel.
Single Tunnel	No Challenge	Cisco VXC traffic receives silent permission to go over the phone VPN with no challenge.

The following table describes how a change in the VXC VPN Option setting alters the operation of the VXC VPN feature when the feature is already enabled.

Table 38: Cisco VXC VPN operation as determined by VXC VPN Option change

VXC VPN action	Result
Change from Dual Tunnel to Single Tunnel	The phone disconnects the VXC VPN tunnel and leaves the phone VPN tunnel intact. Cisco VXC traffic receives permission to go over the phone VPN tunnel.
Change from Single Tunnel to Dual Tunnel	The phone attempts to reuse the phone VPN credentials for the Cisco VXC VPN tunnel silently without considering the VXC Challenge field. If the VPN concentrator is configured for one-time password, the attempt fails and the phone displays the VXC VPN Sign In window, which prompts the user to enter a different password.

Minimum Cisco VXC Firmware Release Required

To support the VXC VPN feature, the Cisco VXC clients must be running the following minimum firmware releases:

- Cisco VXC 2112: ICA Firmware Release 7.1_118
- Cisco VXC 2111: PCoIP Firmware Release 4.0 (Q3CY12)

Additional Cisco VXC VPN Setup Requirements

The following sections describe additional phone configuration that is required to support the Cisco VXC VPN.

Cisco Unified Communications Manager Setup for Cisco VXC VPN

The following Cisco Unified Communications Manager configuration is required to support the Cisco VXC VPN:

PC Port Enabled

You must set the PC Port to Enabled. If the PC port is disabled, the Cisco VXC cannot access the network. The phone provides no enforcement of this configuration.

Span to PC Port Disabled

You must set the Span to PC Port option to Disabled. The Cisco VXC does not require this feature.

You can set the preceding parameters in Cisco Unified Communications Manager Administration by using any of the following configuration windows:

- Phone Configuration window (**Device** > **Phone**)
- Common Phone Profile Configuration window (**Device** > **Device Settings** > **Common Phone Profile**)
- Enterprise Phone Configuration window (**System** > **Enterprise Phone Configuration**)

VPN Concentrator Setup for Cisco VXC VPN

The recommended VPN concentrator for use with this feature is the Cisco ASA 5500 Series Adaptive Security Appliance. To support the Cisco VXC VPN, you must set up the ASA for multisession support so that the phone can establish two tunnels that use the same credentials.

Network Guidelines for Cisco VXC VPN

The following network guidelines exist for the Cisco VXC VPN feature implementation:

- The MTU size in the phone VPN profile is a configurable value. The default value is 1290.
- The maximum MTU value on the phone itself is hardcoded at 1406.
- The MTU value must be no greater than 1406, but it should not be less than 576, because some IIS and virtualization servers do not accept values less than 576.
- You must set up the firewall to allow the MTU value that you specify in the phone VPN profile.
- If the phone cannot download the certificate file or the phone configuration file, check for the allowed packet size in the network.
- If the Cisco VXC VPN cannot establish a tunnel, then ping the VPN concentrator IP address with a packet size (load) to match the MTU value that the VPN profile specifies.
- If the ping fails, try another ping that specifies no load. If the ping still fails without the load, check the routing configuration.
- If the ping fails only with the load included, check the firewall to ensure that it is configured to allow the required MTU.
- Perform a traceroute to the VPN concentrator IP address, and then ping each route with the load to determine the source of the issue.
- Ensure the Don't Fragment (DF) bit is not set on the server, network, or IP phone VPN tunnel.

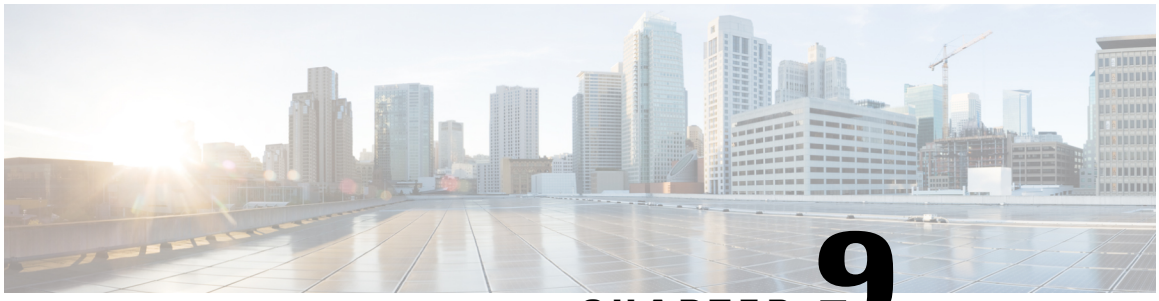
Cisco VXC VPN Limitations and Restrictions

The following limitations and restrictions apply:

- Only Layer 3 packets are tunneled. The Cisco VXC VPN feature does not support Layer 2 tunneling. Therefore any Layer 2 capabilities are lost if the Cisco VXC connects through VPN.
- The VPN client supports only IPv4 addresses.
- The Cisco VXC VPN tunnel cannot be established over a Wi-Fi interface.

- The Enable VXC VPN for MAC feature option is configurable only after you set up the phone VPN parameters, including VPN Group and VPN Profile. This restriction exists because the Cisco VXC VPN can share the same VPN parameters as the phone VPN.
- All existing limitations and restrictions that apply to the phone VPN support apply to the Cisco VXC VPN as well.

Note Do not turn on the VPN before a downgrade to a load previous to 9.2(3), or the phone will be unregistered.



CHAPTER 9

Cisco Unified IP Phone Customization

This chapter explains how you customize configuration files, phone ring sounds, and background images, and how to disable the phone screen to conserve power.

This chapter includes these topics:

Customization and Modification of Configuration Files

You can modify configuration files (for example, edit the xml files) and add customized files (for example, custom ring tones and, call-back tones) to the TFTP directory. You can modify files and add customized files to the TFTP directory in Cisco Unified Communications Operating System Administration from the TFTP Server File Upload window. For information on how to upload files to the TFTP folder on a Cisco Unified Communications Manager server, see *Cisco Unified Communications Operating System Administration Guide*.

You can obtain a copy of the Ringlist.xml and List.xml files from the system by using the following administration command line interface (CLI) *file* commands. For exact syntax, see *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*.

- admin:file
  - file list
  - file view
  - file search

- file get
- file dump
- file tail
- file delete

Custom phone rings

The Cisco Unified IP Phone ships with two default ring types that are implemented in hardware: Chirp1 and Chirp2. Cisco Unified Communications Manager also provides a default set of additional phone ring sounds that are implemented in software as pulse code modulation (PCM) files. The PCM files, along with an XML file (named Ringlist.xml) that describes the ring list options that are available at your site, exist in the TFTP directory on each Cisco Unified Communications Manager server.

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

For more information, see the "Cisco TFTP" chapter in *Cisco Unified Communications Manager System Guide* and the "Software Upgrades" chapter in *Cisco Unified Communications Operating System Administration Guide*.

Ringlist.xml File Format Requirements

The Ringlist.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 Unified 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 Unified 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.xml file that defines two phone ring types:

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

PCM File Requirements for Custom Ring Types

The PCM files for the rings must meet the following requirements for proper playback on Cisco Unified 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.

Set Up Custom Phone Ring

To create custom phone rings for the Cisco Unified IP Phone, perform these steps:

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 PCM File Requirements for Custom Ring Types, on page 213.

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 "Software Upgrades" chapter in *Cisco Unified Communications Operating System Administration Guide*.

Step 3 Use a text editor to edit the Ringlist.xml file. See Ringlist.xml File Format Requirements, on page 212 for information about how to format this file and for a sample Ringlist.xml file.

Step 4 Save your modifications and close the Ringlist.xml file.

Step 5 To cache the new Ringlist.xml file, stop and start the TFTP service by using Cisco Unified Serviceability or disable and reenable the "Enable Caching of Constant and Bin Files at Startup" TFTP service parameter (that is found in the Advanced Service Parameters area.)

Custom Background Images

You can provide users with a choice of background images (or wallpaper) for the LCD screen on their phones. Users can select a background image by choosing **Applications** > **Preferences** > **Wallpaper** on the phone.

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

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

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

For more information, see the "Common Phone Profile Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*.

List.xml File Format Requirements

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

Desktops/640x480x24

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

For more information, see the "Software Upgrades" chapter in *Cisco Unified Communications Operating System Administration Guide*.

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

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

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

List.xml Example

```
<CiscoIPPhoneImageList>
<ImageItem Image="TFTP:Desktops/640x480x24/TN-Fountain.png"
URL="TFTP:Desktops/640x480x24/Fountain.png"/>
<ImageItem Image="TFTP:Desktops/640x480x24/TN-FullMoon.png"
URL="TFTP:Desktops/640x480x24/FullMoon.png"/>
</CiscoIPPhoneImageList>
```

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

PNG File Requirements for Custom Background Images

Each background image requires two PNG files:

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

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

The PNG files for background images must meet the following requirements for proper display on the Cisco Unified IP Phone:

- Full size image - 640 pixels (width) X 480 pixels (height).
- Thumbnail image - 123 pixels (width) X 111 pixels (height).

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

Set Up Custom Background Image

To create custom background images for the Cisco Unified IP Phone, follow these steps.

Procedure

Step 1 Create two PNG files for each image (a full-size version and a thumbnail version). Ensure the PNG files comply with the format guidelines that are listed in PNG File Requirements for Custom Background Images, on page 215.

Step 2 Upload the new PNG files that you created to the following subdirectory in the TFTP server for the Cisco Unified Communications Manager:
Desktops/640x480x24

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

To upload the files, choose **Software Upgrades** > **Upload TFTP Server File** in Cisco Unified Communications Operating System Administration. For more information, see the "Software Upgrades" chapter in *Cisco Unified Communications Operating System Administration Guide*.

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

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

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

Step 4 Use a text editor to edit the List.xml file. See List.xml File Format Requirements, on page 214 for the file location, file, formatting requirements, and a sample file.

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

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

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

Wideband Codec Setup

By default, the G.722 codec is enabled for the Cisco Unified IP Phone 8961, 9951, and 9971. If Cisco Unified Communications Manager is configured to use G.722 and if the far endpoint supports G.722, the call connects using the G.722 codec in place of G.711.

This situation occurs regardless of whether the user has enabled a wideband headset or wideband handset, but if either the headset or handset is enabled, the user may notice greater audio sensitivity during the call. Greater sensitivity means improved audio clarity but also means that the far endpoint can hear more background noise: noise such as rustling papers or nearby conversations. Even without a wideband headset or handset, some users may prefer the additional sensitivity of G.722 distracting. Other users may prefer the additional sensitivity of G.722.

The Advertise G.722 Codec service parameter affects whether wideband support exists for all devices that register with this Cisco Unified Communications Manager server or for a specific phone, depending on the Cisco Unified Communications Manager Administration window where the parameter is configured:

- Advertize G.722 Codec field: From Cisco Unified Communications Manager Administration, choose **System** > **Enterprise Parameters**. The default value of this enterprise parameter is **True**, which means that all Cisco Unified IP Phone Models 9971 that register to this Cisco Unified Communications Manager advertise G.722 to Cisco Unified Communications Manager. If each endpoint in the attempted call supports G.722 in the capabilities set, Cisco Unified Communications Manager chooses that codec for the call whenever possible.
- A specific phone advertises the G.722 codec: From Cisco Unified Communications Manager Administration, choose **Device** > **Phone**. The default value of this product-specific parameter is to use the value that the enterprise parameter specifies. If you want to override this on a per-phone basis, choose **Enabled** or **Disabled** in the Advertise G.722 Codec parameter in the Product Specific Configuration area of the Phone Configuration window.

Idle Display Setup

You can specify an idle display (text only; text file size should not exceed 1M bytes) that appears on the phone screen. The idle display is an XML service that the phone invokes when the phone is idle (not in use) for a designated period and no feature menu is open.

For detailed instructions about creating and displaying the idle display, see *Creating Idle URL Graphics on Cisco Unified IP Phone* at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_tech_note09186a00801c0764.shtml

In addition, see the *Cisco Unified Communications Manager Administration Guide* or the *Cisco Unified Communications Manager Bulk Administration Guide* for the following information:

- Specifying the URL of the idle display XML service:
  - For a single phone: Idle field in the Phone Configuration window in Cisco Unified Communications Manager Administration.
  - For multiple phones simultaneously: URL Idle field in the Enterprise Parameters Configuration window, or the Idle field in the Bulk Administration Tool (BAT)
    - Specifying the length of time that the phone is not used before the idle display XML service is invoked:

- For a single phone: Idle Timer field in the Phone configuration window in Cisco Unified Communications Manager Administration.
- For multiple phones simultaneously: URL Idle Time field in the Enterprise Parameters Configuration window, or the Idle Timer field in the Bulk Administration Tool (BAT)

From a phone, you can see settings for the idle display XML service URL and the length of time that the phone is not used before this service is invoked. To see these settings, choose **Settings** > **Device Configuration** and scroll to the Idle URL and the Idle URL Time parameters.

Automatically Disable Cisco Unified IP Phone Display

To conserve power and ensure the longevity of the phone screen display, set the display to turn off when it is not needed (PowerSave). PowerSave differs from EnergyWise. For more information on EnergyWise, see EnergyWise on the Cisco Unified IP Phone Setup, on page 219.

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.

To turn on the display any time it is off, the phone user presses **Select**.

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

The following table explains the Cisco Unified Communications Manager Administration fields that control when the display turns on and off. Configure these fields in the Product Specific Configuration area of the Phone Configuration window in Cisco Unified Communications Manager Administration. You access this window by choosing **Device** > **Phone** from Cisco Unified Communications Manager Administration.

Table 39: Display On and Off 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.
Display On Time	Time each day that the display turns on automatically (except on the days that the Days Display Not Active field specifies). Enter the time in this field in 24-hour format, where 0:00 is midnight, and use the format *hours:minutes*. For example, to automatically turn the display on at 7:00 a.m. (0700), enter **7:00**. To turn the display on at 2:00 p.m. (1400), enter **14:00**. If this field is blank, the display automatically turns on at 0:00. The default value is 07:30.

Field	Description
Display On Duration	Length of time that the display remains on after turning on at the time that the Display On Time field specifies. 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 **4:30**. If this field is blank, the phone turns 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 remains on continuously. The default value is 10:30.
Display Idle Timeout	Length of time that the phone remains idle before the display turns off. Applies only when the display was powered off as scheduled and was turned on by a user (by pressing **Select** on the phone). 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 **1:30**. The default value is 1:00.

EnergyWise on the Cisco Unified IP Phone Setup

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 timer expires.

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

The following table explains the Cisco Unified Communications Manager Administration fields that control the EnergyWise settings. You configure these fields in Cisco Unified Communications Manager Administration in the Product Specific Configuration area of the Phone Configuration window **Device** > **Phone**.

Table 40: 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. Leaving the Allow EnergyWise Overrides checked with no days selected in the Enable Power Save Plus field does not disable Power Save Plus.
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 7:00 a.m. (0700), enter 7:00. To power up 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 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.

Field	Description
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.
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.

Field	Description
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: 1 One or more days must be selected in the Enable Power Save Plus field. 2 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 checked. Leaving the Allow EnergyWise Overrides checked with no days selected in the Enable Power Save Plus field does not disable Power Save Plus.

SSH Access

You can enable or disable access to the SSH daemon through port 22. Leaving port 22 open leaves the phone vulnerable to Denial of Service (DoS) attacks. By default, the SSH daemon is disabled.

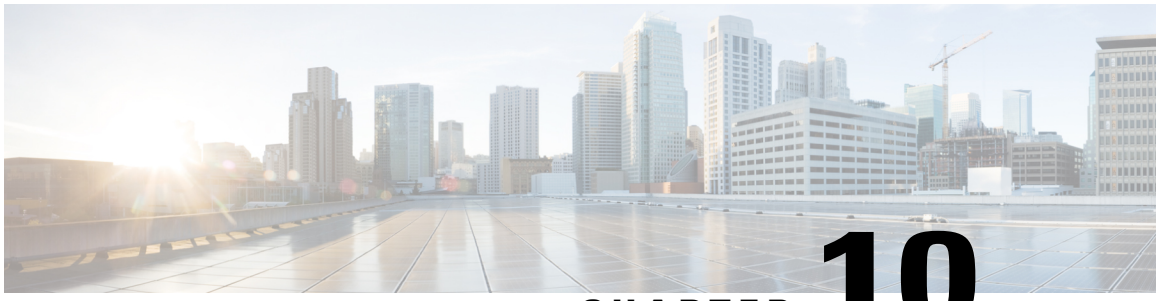
Note Phones that are upgraded from Firmware Release 9.2.0 or earlier to Firmware Release 9.2.1 or later have the SSH Access parameter set to Disabled by default. You must enable the SSH Access parameter before users of these phones can use SSH.

The following table describes the SSH Access field.

- Common Phone Profile Configuration (**Device** > **Device Settings** > **Common Phone Profile**).
- Phone Configuration (**Device** > **Phone windows**).

Table 41: SSH Enable field

Field	Description
SSH Access	Select **Enabled** to allow access to the SSH Daemon. Select **Disabled** to disallow access to the SSH Daemon. The default is Disabled.



CHAPTER 10

Model information, status, and statistics

This chapter describes how to view model information, status messages, and network statistics on the Cisco Unified IP Phone 8961, 9951, and 9971.

- 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. For more information, see Remote Monitoring, on page 247.

For more information about troubleshooting the Cisco Unified IP Phone 8961, 9951, and 9971, see Troubleshooting and Maintenance, on page 267.

This chapter includes these topics:

Display Model Information Screen

To display the Model Information screen, follow these steps.

Procedure

Step 1 Press **Applications** and then select **Phone Information**.
If the user is connected to a secure or authenticated server, a corresponding icon (lock or certificate) displays in the Phone Information Screen to the right of the server option. If the user is not connected to a secure or authenticated server, no icon appears.

The Model Information screen includes the options that are described in Model Information Fields, on page 226.

Step 2 To exit the Model Information screen, press **Exit**.

Model Information Fields

The following table describes the Model Information settings.

Table 42: Model Information settings for the Cisco Unified IP Phone

Option	Description	To change
Model Number	Model number of the phone.	Display only. Cannot configure.
IPv4 Address or IPv6 address	IP address of the phone. The address displayed depends on the IPv6 setup.	Display only. Cannot configure.
Host name	Host name of the phone.	Display only. Cannot configure.
Active Load	Version of firmware currently installed on the phone. The user can press **Details** for more information.	Display only. Cannot configure.
Inactive Load	Inactive Load appears only when a download is in progress. A download icon and a status of "Upgrade in Progress" or "Upgrade Failed" also display. If a user presses **Details** during an upgrade, the download filename and components are listed. A new firmware image can be set to download in advance of a maintenance window. Thus instead of waiting for all of the phones to download the firmware, the system switches more rapidly between resetting an existing load to Inactive status and installing the new load. When the download is complete, the icon changes to indicate the completed status; and a check mark displays for a successful download, or an "X" displays for a failed download. If possible, the rest of the loads continue to download.	Display only. Cannot configure.
Last Upgrade	Date of the most recent firmware upgrade.	Display only. Cannot configure.
Active Server	Domain name of the server to which the phone is registered.	Display only. Cannot configure.
Stand-by Server	Domain name of the standby server.	Display only. Cannot.

Status Menu

The Status menu includes the following options, which provide information about the phone and phone operations:

- Status Messages: Displays the Status Messages screen, which shows a log of important system messages.
- Ethernet Statistic: Displays the Ethernet Statistics screen, which shows Ethernet traffic statistics.
- Wireless Statistics: Displays the Wireless Statistics screen, if applicable.
- Call Statistics: Displays counters and statistics for the current call.
- Current Access Point: Displays the Current Access Point screen, if applicable.

Display Status Menu

To display the Status menu, perform these steps:

Procedure

Step 1 To display the Status menu, press **Applications**.

Step 2 Select **Administrator Settings** > **Status**.

Step 3 To exit the Status menu, press **Exit**.

Status Messages Screen

The Status Messages screen displays the 30 most recent status messages that the phone has generated. You can access this screen at any time, even if the phone has not finished starting up. Status Messages, on page 228 describes the status messages that might appear. This table also includes actions you can take to address errors.

Display Status Messages Screen

To display the Status Messages screen, follow these steps:

Procedure

Step 1 Press **Applications** .

Step 2 Select **Administrator Settings**.

Step 3 Select **Status**.

Step 4 Select **Status Messages**. See Status Messages, on page 228 for a description of the status messages.

Step 5 To remove current status messages, press **Clear List**.

Step 6 To exit the Status Messages screen, press **Exit.**

Status Messages

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

Table 43: Status messages on the Cisco Unified IP Phone

Message	Description	Possible explanation and action
CFG TFTP Size Error	The configuration file is too large for file system on the phone.	Power cycle the phone.
Checksum Error	Downloaded software file is corrupted.	Obtain a new copy of the phone firmware and place it in the TFTPPath directory. You should only copy files into this directory when the TFTP server software is shut down; otherwise, the files may be corrupted.
CTL and ITL installed	The CTL and ITL files are installed on the phone.	None. This message is informational only. Neither the CTL file nor the ITL file was installed previously. For more information about the trust list, see *Cisco Unified Communications Manager Security Guide*.
CTL Installed	A certificate trust list (CTL) file is installed in the phone.	None. This message is informational only. The CTL file was not installed previously. For more information about the CTL file, see the *Cisco Unified Communications Manager Security Guide*.

Message	Description	Possible explanation and action
CTL update failed	The phone could not update the certificate trust list (CTL) file.	Problem with the CTL file on the TFTP server. For more information, see the *Cisco Unified Communications Manager Security Guide*.
DHCP timeout	DHCP server did not respond.	Network is busy - The errors should resolve themselves when the network load reduces. No network connectivity between the DHCP server and the phone - Verify the network connections. DHCP server is down - Check configuration of DHCP server. Errors persist - Consider assigning a static IP address. See the Ethernet Setup menu, on page 104 for details about assigning a static IP address.
DNS timeout	DNS server did not respond.	Network is busy - The errors should resolve themselves when the network load reduces. No network connectivity between the DNS server and the phone - Verify the network connections. DNS server is down - Check configuration of the DNS server.
DNS unknown host	DNS could not resolve the name of the TFTP server or Cisco Unified Communications Manager.	Verify that the host names of the TFTP server or Cisco Unified Communications Manager are configured properly in DNS. Consider using IP addresses rather than host names
Duplicate IP	Another device is using the IP address that is assigned to the phone.	If the phone has a static IP address, verify that you did not assigned a duplicate IP address. See Ethernet Setup menu, on page 104 for details. If you are using DHCP, check the DHCP server configuration.

Message	Description	Possible explanation and action
Erasing CTL and ITL files	Erasing CTL or ITL file.	None. This message is informational only. For more information about the CTL and ITL files, see the *Cisco Unified Communications Manager Security Guide*.
Error update locale	One or more localization files could not be found in the TFTPPath directory or were not valid. The locale was not changed.	From Cisco Unified Operating System Administration, check that the following files are located within subdirectories in the TFTP File Management: • Located in subdirectory with same name as network locale: ◦ tones.xml • Located in subdirectory with same name as user locale: ◦ glyphs.xml ◦ dictionary.xml ◦ kate.xml

Message	Description	Possible explanation and action
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 is created when the phone is added to the Cisco Unified Communications Manager database. If the phone does not exist in the Cisco Unified Communications Manager database, the TFTP server generates a CFG File Not Found response. • Phone is not registered with Cisco Unified Communications Manager. You must manually add the phone to Cisco Unified Communications Manager if you are not allowing phones to autoregister. See Cisco Unified Communications Manager Administration Phone Addition, on page 52 for details. • If you are using DHCP, verify that the DHCP server is pointing to the correct TFTP server. • If you are using static IP addresses, check configuration of the TFTP server. See Ethernet Setup menu, on page 104 for details about assigning a 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 register to Cisco Unified Communications Manager.
IP address released	The phone is configured to release the IP address.	The phone remains idle until it is power cycled or until you reset the DHCP address. See Ethernet Setup menu, on page 104 for details.

Message	Description	Possible explanation and action
ITL installed	The ITL file is installed in the phone.	None. This message is informational only. The ITL file was not installed previously. For more information about the ITL file, see *Cisco Unified Communications Manager Security Guide*.
Load rejected HC	The application that was downloaded is not compatible with the phone hardware.	Occurs if you attempted to install a version of software on this phone that did not support hardware changes on this phone. Check the load ID that is assigned to the phone (from Cisco Unified Communications Manager, choose **Device** > **Phone**). Reenter the load that displays on the phone.
No default router	DHCP or static configuration did not specify a default router.	If the phone has a static IP address, verify that the default router is configured. See Ethernet Setup menu, on page 104 for details. If you are using DHCP, the DHCP server has not provided a default router. Check the DHCP server configuration.
No DNS server IP	A name was specified but DHCP or static IP configuration did not specify a DNS server address.	If the phone has a static IP address, verify that the DNS server is configured. See Ethernet Setup menu, on page 104 for details. If you are using DHCP, the DHCP server has not provided a DNS server. Check the DHCP server configuration.
No Trust List installed	The CTL file or the ITL file is not installed on the phone.	The trust list is not configured on the Cisco Unified Communications Manager, which does not support security by default. For more information about the trust list, see the *Cisco Unified Communications Manager Security Guide*.

Message	Description	Possible explanation and action
Restart requested by Cisco Unified Communications Manager	The phone is restarting due to on a request from Cisco Unified Communications Manager.	Configuration changes were likely made to the phone in Cisco Unified Communications Manager, and **Apply** was pressed so that the changes take effect.
TFTP access error	TFTP server is pointing to a directory that does not exist.	If you are using DHCP, verify that the DHCP server is pointing to the correct TFTP server. If you are using static IP addresses, check configuration of TFTP server. See Ethernet Setup menu, on page 104 for details about assigning a TFTP 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 resolve themselves when the network load reduces. No network connectivity between the TFTP server and the phone - Verify the network connections. TFTP server is down - Check configuration of TFTP server.
Timed Out	Supplicant attempted 802.1X transaction but timed out to due the absence of an authenticator.	Authentication typically times out if 802.1X is not configured 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 and it failed to update the new CTL and ITL files. Possible reasons for failure: • Network failure occurred. • TFTP server was down. • The new security token that was used to sign CTL file and the TFTP certificate that was used to sign ITL file are introduced, but are not available in the current CTL and ITL files in the phone. • Internal phone failure occurred. Possible solutions: • Check network connectivity. • Check whether the TFTP server is active and functioning normally. • If the Transactional Vsam Services (TVS) server is supported on Cisco Unified Communications Manager, check whether the TVS server is active and functioning normally. • Verify whether the security token and the TFTP server are valid. Manually delete the CTL and ITL files if all the preceding solutions fail; reset the phone.
Trust List updated	The CTL file, the ITL file, or both files are updated.	None. This message is informational only. For more information about the trust list, see the *Cisco Unified Communications Manager Security Guide*.
Version error	The name of the phone load file is incorrect.	Make sure that the phone load file has the correct name.

Message	Description	Possible explanation and action
XmlDefault.cnf.xml, or .cnf.xml corresponding to the phone device name	Name of the configuration file.	None. This message indicates the name of the configuration file for the phone.

Display Ethernet Statistics Screen

The Ethernet Statistics screen displays information about the phone and network performance. Ethernet Statistics Information describes the information that appears on this screen.

To display the Ethernet Statistics screen, follow these steps:

Procedure

Step 1 Press **Applications** .

Step 2 Select **Administrator Settings**.

Step 3 Select **Status**.

Step 4 Select **Status** > **Ethernet Statistics**. See Ethernet Statistics Information for a description of the Ethernet statistics.

Step 5 To reset the Rx Frames, Tx Frames, and Rx Broadcasts statistics to 0, press **Clear List**.

Step 6 To exit the Ethernet Statistics screen, press **Exit**.

Ethernet Statistics information

The following tables describe the information in the Ethernet Statistics screen.

Table 44: Ethernet Statistics for the Cisco Unified IP Phone

Item	Description
DHCP state (IPv4 / IPv6)	• In IPv4-mode, displays only the DHCPv4 state, such as DHCP BOUND. • In IPv6-mode, displays only the DHCPv6 state, such as ROUTER ADVERTISE., (GOOD IP). • In dual-stack mode, both DHCPv4 and DHCPv6 state information is displayed. **Draft comment:** Refer them to the tables added in step 3 above

Table 45: DHCPv4 ethernet statistics

DHCPv4 state	Description
CDP INIT	CDP is not bound or WLAN is not in service
DHCP BOUND	DHCPv4 is BOUND
DHCP DISABLED	DHCPv4 is disabled
DHCP INIT	DHCPv4 is INIT
DHCP INVALID	DHCPv4 is INVALID; this is initial state
DHCP RENEWING	DHCPv4 is RENEWING
DHCP REBINDING	DHCPv4 is REBINDING
DHCP REBOOT	DHCPv4 is init-reboot
DHCP REQUESTING	DHCPv4 is requesting
DHCP RESYNC	DHCPv4 is RESYNCH
DHCP WAITING COLDBOOT TIMEOUT	DHCPv4 is booting
DHCP UNRECOGNIZED	Unrecognized DHCPv4 state
DISABLED DUPLICATE IP	Duplicated IPv4 Address
DHCP TIMEOUT	DHCPv4 Timeout
IPV4 STACK TURNED OFF	Phone is in IPv6-only mode with IPv4 Stack turned off
ILLEGAL IPV4 STATE	Illegal IPv4 state and should not happen

Table 46: DHCPv6 ethernet statistics

DHCPv6 State	Description
CDP INIT	CDP is initializing
DHCP6 BOUND	DHCPv6 is BOUND
DHCP6 DISABLED	DHCPv6 is DISABLED
DHCP6 RENEW	DHCPv6 is renewing

DHCPv6 State	Description
DHCP6 REBIND	DHCPv6 is rebinding
DHCP6 INIT	DHCPv6 is initializing
DHCP6 SOLICIT	DHCPv6 is soliciting
DHCP6 REQUEST	DHCPv6 is requesting
DHCP6 RELEASING	DHCPv6 is releasing
DHCP6 RELEASED	DHCPv6 is released
DHCP6 DISABLING	DHCPv6 is disabling
DHCP6 DECLINING	DHCPv6 is declining
DHCP6 DECLINED	DHCPv6 is declined
DHCP6 INFOREQ	DHCPv6 is INFOREQ
DHCP6 INFOREQ DONE	DHCPv6 is INFOREQ DONE
DHCP6 INVALID	DHCPv6 is INVALID; this is initial state
DISABLED DUPLICATE IPV6	DHCP6 is DISABLED, but DUPLICATE IPV6 DETECTED
DHCP6 DECLINED DUPLICATE IP	DHCP6 is DECLINED -- DUPLICATE IPV6 DETECTED
ROUTER ADVERTISE., (DUPLICATE IP)	Duplicated autoconfigured IPv6 address
DHCP6 WAITING COLDBOOT TIMEOUT	DHCPv6 is booting
DHCP6 TIMEOUT USING RESTORED VAL	DHCPv6 timeout, using the value saved in flash memory
DHCP6 TIMEOUT CANNOT RESTORE	DHCP6 timeout and there is no backup from flash memory
IPV6 STACK TURNED OFF	Phone is in IPv4-only mode with IPv6 Stack turned off
ROUTER ADVERTISE., (GOOD IP)	
ROUTER ADVERTISE., (BAD IP)	
UNRECOGNIZED MANAGED BY	IPv6 Address is not from router or DHCPv6 server

DHCPv6 State	Description
ILLEGAL IPV6 STATE	Illegal IPv6 state and should not happen

Draft comment: ----------End Chunk 8 (AG)----------

Display Wireless Statistics Screen

The Wireless Statistics screen displays statistics about the wireless Cisco Unified IP Phone 9971.

To display the Wireless Statistics screen, follow these steps:

Procedure

Step 1 Press **Applications** .

Step 2 Select **Administrator Settings**.

Step 3 Select **Status**.

Step 4 Select **Wireless Statistics**. See Wireless Statistics, on page 238 for a description of the Wireless statistics.

Step 5 To reset the Wireless statistics to 0, press **Clear List**.

Step 6 To exit the Wireless Statistics screen, press **Exit**.

Wireless Statistics

The following table describes the Wireless statistics on the phone.

Table 47: Wireless Statistics on the Cisco Unified IP Phone

Item	Description
Transmit Frames	Number of packets that the phone transmitted.
Directed Frames Received	Number of directed packets that the phone received.
Multicast Frames Received	Number of multicast packets that the phone received.
Broadcast Frames Received	Number of broadcast packets that the phone received.
Receive Errors	Number of packets with errors that the phone received.
Receive No Buffers	The phone has no buffers available to receive the packet.
Frame Checksum (FCS) Errors	Increments when an FCS error is detected in a received MPDU.

Item	Description
Duplicate Frames	Number of duplicate packets received by the phone.
Fragments Received	Number of fragmented packets that the phone received.
Beacons Received	Number of beacons that the phone received.
Association Rejected	Number of AP association rejections that the phone received.
Association Timeouts	Number of AP association timeouts that the phone received.
Authentication Rejects	Number of authentication rejects that the phone received.
Authentication Timeouts	Number of authentication timeouts that the phone received.
QOS Null Frames	Number of QOS null packets that the phone received.
The following Wireless Statistics items display these AP queues: Background (BK), Best Effort (BE), Video (VI), and Voice (VO)	
QOS Data Received	Number of QOS packets that the phone received.
Transmit Ok	Number of packets that the phone transmitted without error.
Transmit Errors	Number of packets with errors that the phone transmitted.
Direct Frames Transmitted	Number of direct packets that the phone transmitted.
Multicast Frames Transmitted	Number of multicast packets that the phone transmitted.
Broadcast Frames Transmitted	Number of broadcast packets that the phone transmitted.
RTS Failed	A corresponding CTS was not received.
ACK Failed	AP did not acknowledge a transmission.
Retries	Counter of total retries.
Multiple Retries	Transmission of packet required two or more retries before success.
Retry Failures	Transmission of packet failed.
Transmit Timeouts	Transmission of packet failed due to queue time.
Success Counter	Counter of successful transmissions.
Max Retry Failure	Counter of successive transmission failures that caused a roaming attempt.

Display Call Statistics Screen

You can access the Call Statistics screen on the phone to display counters, statistics, and voice-quality metrics of the most recent call.

Note You can also remotely view the call statistics information by using a web browser to access the Streaming Statistics web page. This web page contains additional RTCP statistics that are not available on the phone. For more information about remote monitoring, see Remote Monitoring, on page 247.

A single call can use multiple voice streams, but data is captured for only the last voice stream. A voice stream is a packet stream between two endpoints. If one endpoint is put on hold, the voice stream stops even though the call is still connected. When the call resumes, a new voice packet stream begins, and the new call data overwrites the former call data.

To display the Call Statistics screen for information about the latest voice stream, follow these steps:

Procedure

Step 1 Press **Applications**.

Step 2 Select **Administrator Settings**.

Step 3 Select **Status**.

Step 4 Select **Call Statistics**. See Call Statistics, on page 240 for a description of the Call Statistics fields.

Step 5 To exit the Call Statistics screen, press **Exit**.

Call Statistics

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

Table 48: Call Statistics items for the Cisco Unified Phone

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

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.
Rcvr 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	
MOS LQK	Score that is an objective estimate of the mean opinion score (MOS) for listening quality (LQK) that rates from 5 (excellent) to 1 (bad). This score is based on audible concealment events due to frame loss in the preceding eight-second interval of the voice stream. For more information, see Voice Quality Monitoring, on page 293. **Note** The MOS LQK score can vary based on the type of codec that the Cisco Unified IP Phone uses.
Avg MOS LQK	Average MOS LQK score that was observed for the entire voice stream.
Min MOS LQK	Lowest MOS LQK score that was observed from the start of the voice stream.
Max MOS LQK	Baseline or highest MOS LQK score that was observed from start of the voice stream. These codecs provide the following maximum MOS LQK score under normal conditions with no frame loss: • G.711 yields a score of 4.5. • G.729 A /AB yields a score of 3.7.

Item	Description
MOS LQK Version	Version of the Cisco proprietary algorithm that is used to calculate MOS LQK scores.
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 Secs	Number of seconds that have concealment events (lost frames) from the start of the voice stream (includes severely concealed seconds).
Severely Conceal Secs	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.

Display Video Statistics Screen

You can access the Video Statistics screen on the phone to display counters, statistics of the most recent call.

Note You can also remotely view the video statistics information by using a web browser to access the Streaming Statistics web page. This web page contains additional RTCP statistics that are not available on the phone. For more information about remote monitoring, see Remote Monitoring, on page 247.

A video stream is a frame stream between two endpoints. If one endpoint pauses the video streaming, the video stream stops even though the call is still connected. When the video streaming resumes, a new video frame stream begins, and the new video data overwrites the former video data.

To display the Video Statistics screen for information about the latest video stream, follow these steps:

Procedure

Step 1 Press **Applications** .

Step 2 Select **Administrator Settings**.

Step 3 Select **Call Statistics**.

Step 4 Select **Video**. See Video Statistics, on page 243 for a description of the Video statistics.

Step 5 To exit the Video screen, press **Exit**.

Video Statistics

The following table describes the Video Statistics fields.

Table 49: Video Statistics items for the Cisco Unified Phone

Item	Description
Rcvr Codec	Type of received video stream (RTP streaming video from codec).
Sender Codec	Type of transmitted video stream (RTP streaming video from codec).
Rcvr Packets	Number of RTP video packets that were received since the video stream opened. **Note** This number is not necessarily identical to the number of RTP video packets received since the call began because the call might have been placed on hold.
Sender Packets	Number of RTP video packets that were transmitted since the video stream opened. **Note** This number is not necessarily identical to the number of RTP video packets 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 video stream opened.
Max Jitter	Maximum jitter, in milliseconds, observed since the receiving video stream opened.
Rcvr Discarded	Number of RTP packets in the receiving video stream that were discarded (bad packets, too late, and so on).
Rcvr Lost Packets	Missing RTP video packets (lost in transit).
Rcvr Size	Size of video frames, in milliseconds, in the receiving video stream (RTP streaming video).
Sender Size	Size of video frames, in milliseconds, in the transmitting video stream.
Sender Frames	Number of video frames that by the camera/phone transmitted since the video stream opened.
Sender Partial Frames	Number of P-frames that the camera sent since the video stream opened.
Sender IFrames	Number of I-frames that the camera sent since the video stream opened.

Item	Description
Sender Frame Rate	Rate at which video frames are transmitted (in frames per second).
Sender Bandwidth	Bandwidth of the transmitted video steam in kbps (kilo bits per second).
Sender Resolution	Resolution of the video stream that the camera transmits. VGA(640x480), CIF (352x288), QCIF (176x144)
Rcvr Frames	Number of video frames that the phone received since the video stream opened.
Rcvr Partial Frames	Number of P-frames that the phone received since the video stream opened.
Rcvr IFrames	Number of I-frames that the phone received since the video stream opened.
Rcvr IFrames Req	Number of IDR requests that the phone sent to the remote endpoint since the video stream opened.
Rcvr Frame Rate	Rate at which video frames are received (in frames per second).
Rcvr Frame Errors	Number of errors that the video decoder reported since the video stream opened.
Rcvr Bandwidth	Bandwidth of the received video steam in kbps (kilo bits per second).
Rcvr Resolution	Resolution of the video stream that the phone received from the remote endpoint. VGA(640x480), CIF (352x288), QCIF (176x144), and so forth.
Sender Start Time	Time stamp that indicates when the first RTP packet is sent to the network.
Rcvr Start Time	Time stamp that indicates when the first RTP packet is received from the network.
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.

Display Current Access Point Screen

The Current Access Point screen displays statistics about the current access point on the wireless Cisco Unified IP Phone 9971. Current Access Point, on page 245 describes the information that appears in this screen.

To display the Current Access Point screen, follow these steps:

Procedure

Step 1 Press **Applications** .

Step 2 Select **Administrator Settings**.

Step 3 Select **Status**.

Step 4 Select **Current Access Point**.

Step 5 To exit the Current Access Point screen, press **Exit**.

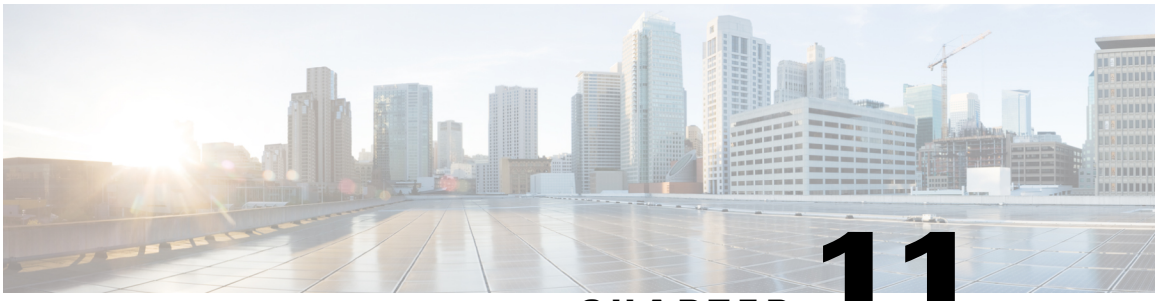
Current Access Point

The following table describes the fields in the Current Access Point screen.

Table 50: Current Access Point items on the Cisco Unified IP Phone 9971

Item	Description
AP Name	Name of the AP, if it is CCX-compliant; otherwise, the MAC address displays here.
MAC Address	MAC address of the AP.
Frequency	The latest frequency where this AP was observed.
Last RSSI	The latest RSSI in which this AP was observed.
Beacon Interval	Number of time units between beacons. A time unit is 1.024 ms.
Capability	This field contains a number of subfields that are used to indicate requested or advertised optional capabilities.
Basic Rates	Data rates that the AP requires and the AP at which the station must be capable of operating.
Optional Rates	Data rates that the AP supports and the AP that are optional for the station to operate at.
Current Channel	The latest channel where this AP was observed.
dtime Period	Every nth beacon is a dtime period. After each DTIM beacon, the AP sends any broadcast or multicast packets that are queued for power-save devices.
Country Code	A two-digit country code. Country information might not be display if the country information element (IE) is not present in the beacon.
Channels	A list of supported channels (from the country IE).

Item	Description
Power Constraint	The amount of power by which the maximum transmit power should be reduced from the regulatory domain limit.
Power Limit	Maximum transmit power in dBm that is permitted for that channel.
Channel Utilization	The percentage of time, normalized to 255, in which the AP sensed the medium was busy, as indicated by the physical or virtual carrier sense (CS) mechanism.
Station Count	Data rates that the AP requires and at which the station must be capable of operating.
Admission Capacity	An unsigned integer that specifies the remaining amount of medium time that is available through explicit admission control, in units of 32 microseconds per second. If the value is 0, the AP does not support this information element and the capacity is unknown.
WMM Supported	Support for Wi-Fi multimedia extensions.
UAPSD Supported	The AP supports Unscheduled Automatic Power Save Delivery. May only be available if WMM is supported. This feature is critical for talk time and for achieving maximum call density on the wireless IP Phone.
Proxy ARP	CCX-compliant AP supports responding to IP ARP requests on behalf of the associated station. This feature is critical to standby time on the wireless IP Phone.
CCX Version	If the AP is CCX compliant, this field shows the CCX version.



CHAPTER 11

Remote Monitoring

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

- 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.

You can also request line information from the phone and get a report in XML format.

You can also obtain much of this information directly from a phone. For more information, see Model information, status, and statistics, on page 225.

For more information about troubleshooting the Cisco Unified IP Phone, see Troubleshooting and Maintenance, on page 267.

This chapter includes these topics:

Access Web Page for Phone

To access the web page for a Cisco Unified IP Phone, follow these steps:

Note If you cannot access the web page, it may be disabled by default. For more information, see Control web page access, on page 249.

Procedure

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

a) Search for the phone in Cisco Unified Communications Manager Administration by choosing **Device** > **Phone**. Phones that register with Cisco Unified Communications Manager display the IP address on the Find and List Phones window and at the top of the Phone Configuration window.

b) On the Cisco Unified IP Phone, press **Applications**, choose **Administrator Settings** > **Network Setup** > **Ethernet Setup** > **IPv4 Setup**, and then scroll to the IP Address option.

Step 2 Open a web browser and enter the following URL, where *IP_address* is the IP address of the Cisco Unified IP Phone:
http://<IP_address> or **https://**<IP_address> (depending on the protocol supported by the Cisco Unified IP Phone)

Cisco Unified IP Phone Web Page Information

The web page for a Cisco Unified IP Phone includes these topics:

- 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: Includes the following hyperlinks, which provide information about network traffic:
  - Ethernet Information: Displays information about Ethernet traffic.
  - Access: Displays information about network traffic to and from the PC port on the phone.
  - Network: Displays information about network traffic to and from the network port on the phone.
- Device Logs: Includes the following hyperlinks, which provide information that you can use for troubleshooting:
  - Console Logs: Includes hyperlinks to individual log files.
  - Core Dumps: Includes hyperlinks to individual dump files.
  - Status Messages: Displays the 10 most recent status messages that the phone has generated since it last powered up.

- Debug Display: Displays debug messages that might be useful to Cisco TAC if you require assistance with troubleshooting.

- Streaming Statistics: Includes the Audio and Video statistics, Stream 1, Stream 2, Stream 3, Stream 4, Stream 5 and Stream 6 hyperlinks, which display a variety of streaming statistics.

Related Topics

Device Information, on page 250
Network Setup, on page 251
Network Statistics, on page 255
Device Logs, on page 258
Streaming Statistics, on page 259

Control web page access

For security purposes, access to the web pages for a phone is disabled by default. This practice prevents access to the web pages that are described in this chapter and to the Cisco Unified Communications Manager User Options web pages.

Note Some features, such as Cisco Quality Report Tool, do not function properly without access to the phone web pages. Disabling web access also affects any serviceability application that relies on web access, such as CiscoWorks.

To enable or disable access to the web pages for a phone, perform these steps from Cisco Unified Communications Manager Administration:

Procedure

Step 1 Choose **Device** > **Phone**.
Step 2 Specify the criteria to find the phone and select **Find**, or select **Find** to display a list of all phones.
Step 3 Select the device name to open the Phone Configuration window for the device.
Step 4 Scroll to the Product Specific Configuration area.
Step 5 To enable access, from the Web Access drop-down list, choose **Enabled**.
Step 6 To disable access, from the Web Access drop-down list, choose **Disabled**.
Step 7 Select **Apply Config**.

Cisco Unified IP Phone and HTTP or HTTPS Protocols

The Cisco Unified IP Phone can be configured to use:

- HTTPS protocol only

- HTTP or HTTPS protocols

If your Cisco Unified IP Phone is configured to use the HTTP or HTTPS protocols, use **http://**<IP_address> or **https://**<IP_address> for phone web access.

If your Cisco Unified IP Phone is configured to use only HTTPS protocol, use **https://**<IP_address> for phone web access.

Device Information

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

Note Some of the items in the following table do not apply to all phone models.

To display the Device Information area, access the web page for the phone as described in Access Web Page for Phone, on page 248, and then click the **Device Information** hyperlink.

Table 51: Device Information Area Items

Item	Description
MAC Address	Media Access Control (MAC) address of the phone.
Host Name	Unique, fixed name that is automatically assigned to the phone based on the MAC address.
Phone DN	Directory number that is assigned to the phone.
Version	Identifier of the firmware that is running on the phone.
Key Expansion Module 1	Identifier for the first KEM, if applicable.
Key Expansion Module 2	Identifier for the second KEM, if applicable.
Key Expansion Module 3	Identifier for the third KEM, if applicable.
Hardware Revision	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.

Item	Description
UDI	Displays the following Cisco Unique Device Identifier (UDI) information about the phone: • Device Type: Indicates hardware type. For example, phone displays for all phone models. • Device Description: Displays the name of the phone associated with the indicated model type. • Product Identifier: Specifies the phone model. • Serial Number: Displays the unique serial number of the phone.
Key Expansion Module UDI	Cisco Unique Device Identifier (UDI) of the KEM.
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.
FIPS Mode Enabled	Indicates if the Federal Information Processing Standard (FIPS) Mode is enabled.

Network Setup

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 Unified IP Phone. For more information, see Cisco Unified IP Phone Settings, on page 101.

To display the Network Setup area, access the web page for the phone as described in Access Web Page for Phone, on page 248, and then click the **Network Setup** hyperlink.

Table 52: Network Setup area items

Item	Description
DHCP Server	IP address of the Dynamic Host Configuration Protocol (DHCP) server from which the phone obtains the IP address.
BOOTP Server	Indicates whether the phone obtains the configuration from a Bootstrap Protocol (BootP) server.
MAC Address	Media Access Control (MAC) address of the phone.

Item	Description
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.
IP Address	Internet Protocol (IP) address of the phone.
Subnet Mask	Subnet mask that the phone uses.
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.
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 servers (DNS Server 2 and 3) that the phone uses.
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.
CUCM Server 1–5	Host names or IP addresses, in prioritized order, of the Cisco Unified Communications Manager servers with which the phone can register. An item can also show the IP address of an SRST router that is capable of providing limited Cisco Unified Communications Manager functionality, if such a router is available. For an available server, an item shows the Cisco Unified Communications Manager server IP address and one of the following states: • Active: Cisco Unified Communications Manager server from which the phone is currently receiving call-processing services • Standby: Cisco Unified Communications Manager server to which the phone switches if the current server becomes unavailable • Blank: No current connection to this Cisco Unified Communications Manager server An item may also include the Survivable Remote Site Telephony (SRST) designation, which identifies an SRST router capable of providing Cisco Unified Communications Manager functionality with a limited feature set. This router assumes control of call processing if all other Cisco Unified Communications Manager servers become unreachable. The SRST Cisco Unified Communications Manager always appears last in the list of servers, even if it is active. You configure the SRST router address in the Device Pool section in Cisco Unified Communications Manager Configuration window.
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.

Item	Description
Messages URL	URL of the server from which the phone obtains message services.
Services URL	URL of the server from which the phone obtains Cisco Unified IP Phone services.
DHCP Enabled	Indicates whether the phone uses DHCP.
DHCP Address Released	Indicates the setting of the DHCP Address Released option on the phone Network Configuration menu.
Alternate TFTP	Indicates whether the phone is using an alternative TFTP server.
Idle URL	URL that the phone displays when the phone is idle for the time that the Idle URL Time field specifies 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 that the Idle URL specifies activates.
Proxy Server URL	URL of proxy server, which makes HTTP requests to nonlocal host addresses on behalf of the phone 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
PC 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 PC port

Item	Description
TFTP Server 2	Backup TFTP server that the phone uses if the primary TFTP server is unavailable.
User Locale	User locale that associates with the phone user. Identifies a set of detailed information to support users, including language, font, date and time formatting, and alphanumeric keyboard text information.
Network Locale	Network locale that associates with the phone user. Identifies a set of detailed information to support the phone in a specific location, including definitions of the tones and cadences that the phone uses.
Headset Enabled	Indicates whether the Headset button is enabled on the phone.
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.
PC Port Disabled	Indicates whether the PC port on the phone is enabled or disabled.
Speaker Enabled	Indicates whether the speakerphone is enabled on the phone.
GARP Enabled	Indicates whether the phone learns MAC addresses from Gratuitous ARP responses.
Video Capability Enabled	Indicates whether the phone can participate in video calls when it connects to an appropriately equipped camera.
Voice VLAN Enabled	Indicates whether the phone allows a device that is attached to the PC port to access the Voice VLAN.
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.
Span to PC Port	Indicates whether the phone forwards packets that are transmitted and received on the network port to the access port.
PC VLAN	VLAN that identifies and removes 802.1P/Q tags from packets that are sent to the PC.

Item	Description
CDP on PC Port	Indicates whether CDP is supported on the PC port (default is enabled). When CDP is disabled in Cisco Unified Communications Manager, a warning is displays to indicate that disabling CDP on the PC port prevents CVTA from working. The current PC and switch port CDP values are shown in the Settings menu.
CDP on 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, indicating that CDP should be disabled on the switch port only if the phone connects to a non-Cisco switch. 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 enabled on the switch port.
LLDP: PC Port	Indicates whether Link Layer Discovery Protocol (LLDP) is enabled on the PC port.
LLDP Power Priority	Advertises the phone power priority to the switch, thus enabling the switch to appropriately provide 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.

Network Statistics

The following Network Statistics hyperlinks on a phone web page provide information about network traffic on the phone:

- Ethernet Information: Displays information about Ethernet traffic.
- Access area: Displays information about network traffic to and from the PC port on the phone.
- Network area: Displays information about network traffic to and from the network port on the phone.

To display a network statistics area, access the web page for the phone, and then click the **Ethernet Information**, the **Access**, or the **Network** hyperlink.

Related Topics

Access Web Page for Phone, on page 248

Ethernet Information Web Page

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

Table 53: 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.

Access Area and Network Area Web Pages

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

Table 54: Access Area and Network Area Items

Item	Description
Rx totalPkt	Total number of packets that the phone received.
Rx crcErr	Total number of packets that were received with CRC failed.
Rx alignErr	Total number of packets between 64 and 1522 bytes in length that were received and that have a bad Frame Check Sequence (FCS).
Rx multicast	Total number of multicast packets that the phone received.

Item	Description
Rx broadcast	Total number of broadcast packets that the phone received.
Rx unicast	Total number of unicast packets that the phone received.
Rx shortErr	Total number of received FCS error packets or Align error packets that are less than 64 bytes in size.
Rx shortGood	Total number of received good packets that are less than 64 bytes size.
Rx longGood	Total number of received good packets that are greater than 1522 bytes in size.
Rx longErr	Total number of received FCS error packets or Align error packets that are greater than 1522 bytes in size.
Rx size64	Total number of received packets, including bad packets, that are between 0 and 64 bytes in size.
Rx size65to127	Total number of received packets, including bad packets, that are between 65 and 127 bytes in size.
Rx size128to255	Total number of received packets, including bad packets, that are between 128 and 255 bytes in size.
Rx size256to511	Total number of received packets, including bad packets, that are between 256 and 511 bytes in size.
Rx size512to1023	Total number of received packets, including bad packets, that are between 512 and 1023 bytes in size.
Rx size1024to1518	Total number of received packets, including bad packets, that are between 1024 and 1518 bytes in size.
Rx tokenDrop	Total number of packets that were dropped due to lack of resources (for example, FIFO overflow).
Tx excessDefer	Total number of packets that were delayed from transmitting due to busy medium.
Tx lateCollision	Number of times that collisions occurred later than 512 bit times after the start of packet transmission.
Tx totalGoodPkt	Total number of good packets (multicast, broadcast, and unicast) that the phone received.
Tx Collisions	Total number of collisions that occurred while a packet was transmitted.
Tx excessLength	Total number of packets that were not transmitted because the packet experienced 16 transmission attempts.

Item	Description
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 protocol discovered.
CDP Neighbor Port	Neighbor device port to which the phone is connected discovered by CDP protocol.
LLDP Neighbor Device ID	Identifier of a device connected to this port discovered by LLDP discovered.
LLDP Neighbor IP Address	IP address of the neighbor device that LLDP protocol discovered.
LLDP Neighbor Port	Neighbor device port to which the phone connects that LLDP protocol discovered.
Port Information	Speed and duplex information.

Device Logs

The following device log hyperlinks on a phone web page provide information that helps to monitor and troubleshoot the phone. To access a device log area, access the web page for the phone as described in Access Web Page for Phone, on page 248.

- 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. The Status Messages screen on the phone also displays this information. Status Messages, on page 228 describes the status messages that can appear.
- Debug Display - Displays debug messages that might be useful to Cisco TAC if you require assistance with troubleshooting.

Streaming Statistics

A Cisco Unified IP Phone can stream information to and from up to three 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 as described in Access Web Page for Phone, on page 248, and then click a Stream hyperlink.

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

Table 55: Streaming Statistics area items

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 that the 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 address.
Sender Packets	Total number of RTP data packets that the phone transmitted since it started this connection. The value is 0 if the connection is set to receive-only mode.
Sender Octets	Total number of payload octets that the phone transmitted in RTP data packets since it started 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.

Item	Description
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 this connection. Defined as the number of expected packets less the number of packets actually received, where the number of received packets includes any that are late or are duplicates. The 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 milliseconds. The value displays as 0 if the connection was set to send-only mode.
Rcvr Codec	Type of audio encoding that is used for the received stream.
Rcvr Reports Sent (see note)	Number of times the RTCP Receiver Reports have been sent.
Rcvr 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 started on this connection. Includes packets that were received from different sources if this call is a 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 reception started on the connection. Includes packets that were received from different sources if this call is a multicast call. The value displays as 0 if the connection was set to send-only mode.
Cumulative Conceal Ratio	Total number of concealment frames divided by total number of speech frames that were received from the start of the voice stream.
Interval Conceal Ratio	Ratio of concealment frames to speech frames in the preceding 3-second interval of active speech. If voice activity detection (VAD) is in use, a longer interval might be required to accumulate three seconds of active speech.
Max Conceal Ratio	Highest interval concealment ratio from the start of the voice stream.
MOS LQK	Score that is an objective estimate of the mean opinion score (MOS) for listening quality (LQK) that rates from 5 (excellent) to 1 (bad). This score is based on audible concealment events that are to frame loss in the preceding eight-second interval of the voice stream. For more information, see Voice Quality Monitoring, on page 293. **Note** The MOS LQK score can vary due to the codec type that the Cisco Unified IP Phone uses.

Item	Description
Avg MOS LQK	Average MOS LQK score that was observed for the entire voice stream.
Min MOS LQK	Lowest MOS LQK score that was observed from the start of the voice stream.
Max MOS LQK	Baseline or highest MOS LQK score that was observed from start of the voice stream. These codecs provide the following maximum MOS LQK score under normal conditions with no frame loss: • G.711 yields 4.5. • G.729 A /AB yields 3.7.
MOS LQK Version	Version of the Cisco proprietary algorithm that is used to calculate MOS LQK scores.
Conceal Secs	Number of seconds that have concealment events (lost frames) from the start of the voice stream (includes severely concealed seconds).
Severely Conceal Secs	Number of seconds that have more than five percent concealment events (lost frames) from the start of the voice stream.
Latency (see note)	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.
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.
Rcvr Size	RTP packet size, in milliseconds, for the received stream.
Rcvr Discarded	RTP packets that were received from the network but were discarded from the jitter buffers.
Rcvr Reports Received (see note)	Number of times RTCP Receiver Reports have been received.

Item	Description
Rcvr Report Time Received (see note)	Most recent time when an RTCP Receiver Report was received.
Voice Quality Metrics	
Cumulative Conceal Ratio	Total number of concealment frames divided by total number of speech frames that were received from the start of the voice stream.
Interval Conceal Ratio	Ratio of concealment frames to speech frames in preceding three-second interval of active speech. If voice activity detection (VAD) is in use, 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 Secs	Number of seconds that have concealment events (lost frames) from the start of the voice stream (includes severely concealed seconds).
Severely Conceal Secs	Number of seconds that have more than five percent concealment events (lost frames) from the start of the voice stream.

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

Related Topics

Cisco Unified IP Phone Settings, on page 101

Request information from 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 a list of the related information for a specific line.
- LineInfo is a list of related information on the configured phone line.
- ModelInfo is a list of the related information about the phone.

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/ModelInfo 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.

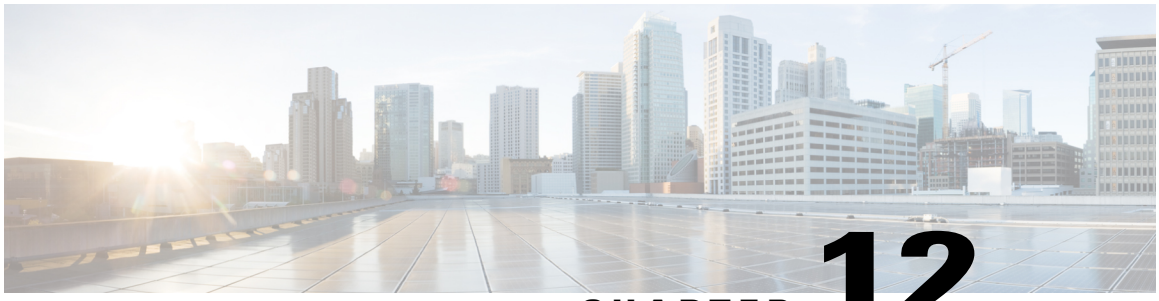
```
<CiscoIPPhoneLineInfo>
   <Prompt/>
   <Notify/>
   <Status>null</Status>
   <CiscoIPPhoneLines>
     <LineType>9</LineType>
     <lineDirNum>1028</lineDirNum>
     <MessageWaiting>NO</MessageWaiting>
     <RingerName>Chirp1</RingerName>
     <LineLabel/>
     <LineIconState>ONHOOK</LineIconState>
   </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 ModelInfo output

The following XML code is an example of the output from the ModelInfo 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

Troubleshooting and Maintenance

This chapter provides information that can assist you in troubleshooting problems with your Cisco Unified IP Phone or with your IP telephony network. The chapter also explains how to maintain your voice network and clean your phone.

If you need additional assistance to resolve an issue, see Documentation, support, and security guidelines, on page xxii.

This chapter includes these topics:

Troubleshooting

Use the following sections to troubleshoot problems with the phones:

Startup Problems

After you install a Cisco Unified IP Phone into your network and add it to Cisco Unified Communications Manager, the phone should start up as described in Phone Startup Verification, on page 68.

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

Cisco Unified IP Phone Does Not Go Through Normal Startup Process

Problem

When you connect a Cisco Unified IP Phone to the network port, the phone does not go through the normal startup process as described in Phone Startup Verification, on page 68 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 Unified IP Phone from another port and connect it to this network port to verify that the port is active.
  - Connect the Cisco Unified IP Phone that does not start up to a different network port that is known to be good.
  - Connect the Cisco Unified 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 with the handset off-hook. When the phone is powered up in this way, it attempts to launch a backup software image.
- If the phone still does not start up properly, perform a factory reset of the phone. For instructions, see Basic Reset, on page 290.
- After you attempt these solutions, if the phone screen on the Cisco Unified IP Phone does not display any characters after at least five minutes, contact a Cisco technical support representative for additional assistance.

Cisco Unified 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 General Troubleshooting Information, on page 289 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 Status Messages Screen, on page 227 for instructions about accessing status messages and for a list of potential errors, their explanations, and their solutions.

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

Problem

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

Solution

Ensure that the network is currently running.

TFTP Server Settings

Problem

The TFTP server settings may not be correct.

Solution

Check the TFTP settings. See Check TFTP settings, on page 284.

IP Addressing and Routing

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. See Check DHCP settings, on page 285.

DNS Settings

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. See Verify DNS settings, on page 287.

Cisco CallManager and TFTP Services Are Not Running

Problem

If the Cisco CallManager 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 CallManager 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 287.

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. See Create new phone configuration file, on page 286.

Cisco Unified Communications Manager Phone Registration

Problem

The phone is not registered with the Cisco Unified Communications Manager

Solution

A Cisco Unified 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 Cisco Unified Communications Manager Phone Addition Methods, on page 50 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 Cisco Unified IP Phone MAC Address Determination, on page 52.

If the phone is already in the Cisco Unified Communications Manager database, the configuration file may be damaged. See Configuration File Corruption, on page 270 for assistance.

Cisco Unified 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.

Cisco Unified IP Phone Resets Unexpectedly

If users report that their phones are resetting during calls or while the phones are idle on their desk, you should investigate the cause. If the network connection and Cisco Unified Communications Manager connection are stable, a Cisco Unified IP Phone should not reset.

Typically, a phone resets if it has problems in connecting to the Ethernet network or to Cisco Unified Communications Manager. These sections can help you identify the cause of a phone resets in your network:

Intermittent network outages

Problem

Your network may be experiencing intermittent outages.

Solution

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

DHCP Setting Errors

Problem

The DHCP settings may be incorrect.

Solution

Verify that you have properly configured the phone to use DHCP. See Ethernet Setup menu, on page 104 for more information. Verify that the DHCP server is set up properly. Verify the DHCP lease duration. Cisco recommends that you set it to 8 days.

Static IP address settings errors

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. See Ethernet Setup menu, on page 104 for more information.

Voice VLAN setup errors

Problem

If the Cisco Unified IP 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.

Phones have not been intentionally reset

Problem

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

Solution

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

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

DNS or other connectivity errors

Problem

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

Solution

If the phone continues to reset, eliminate DNS or other connectivity errors by following the procedure in Determine DNS or connectivity issues, on page 284.

Power Connection Problems

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.

Physical Connection Problems

Problem

The physical connection to the LAN may be broken.

Solution

Verify that the Ethernet connection to which the Cisco Unified 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 Unified IP Phone Security Problems

The following sections provide troubleshooting information for the security features on the Cisco Unified 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 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.

802.1X Authentication Problems

801.1X authentication problems can be broken into the categories that are described in the following table.

Table 56: Identifying 802.1X authentication problems

If all the following conditions apply	See
• Phone cannot obtain a DHCP-assigned IP address. • Phone does not register with Cisco Unified Communications Manager. • Phone status displays `Configuring IP` or `Registering`. • 802.1X Authentication Status displays "Held." • Status menu 802.1X status displays "Failed."	802.1X Is Enabled on Phone but Phone Does Not Authenticate, on page 276
• Phone cannot obtain a DHCP-assigned IP address. • Phone does not register with Cisco Unified Communications Manager. • Phone status displays `Configuring IP` or `Registering`. • 802.1X Authentication Status displays "Disabled", • Status menu displays the DHCP status as timed out.	802.1X Is Not Enabled, on page 277
• Phone cannot obtain a DHCP-assigned IP address. • Phone does not register with Cisco Unified Communications Manager. • Phone status display as `Configuring IP` or `Registering` • You are unable to access phone menus to verify 802.1X status.	Factory Reset of Phone Has Deleted 802.1X Shared Secret, on page 277

802.1X Is Enabled on Phone but Phone Does Not Authenticate

Problem

The phone cannot authenticate.

Cause

These errors typically indicate that 802.1X authentication is enabled on the phone, but the phone is unable to authenticate.

Solution

To resolve this problem, check the 802.1X and shared secret configuration. See Identify 802.1X authentication problems, on page 286.

802.1X Is Not Enabled

Problem

The phone does not have 802.1X configured.

Cause

These errors typically indicate that 802.1X authentication is not enabled on the phone.

Solution

If 802.1X is not enabled on the phone, see 802.1X Authentication and Transaction Status, on page 125.

Factory Reset of Phone Has Deleted 802.1X Shared Secret

Problem

After a reset, the phone does not authenticate.

Cause

These errors typically indicate that the phone has completed a factory reset (see Basic Reset, on page 290) while 802.1X was enabled. A factory reset deletes the shared secret, which is required for 802.1X authentication and network access.

Solution

To resolve this situation, temporarily move the phone to a network environment that is not using 802.1X authentication. After the phone starts up normally, access the 802.1X configuration menus to enable device authentication and to reenter the shared secret (see 802.1X Authentication and Transaction Status, on page 125).

Camera, audio, and video problems

The following sections describe how to resolve camera, audio, and video problems.

No Video

Problem

The phone does not detect the camera or no picture appears on the screen.

Solution

Check the following conditions:

- Verify that the camera is connected properly by unplugging and reconnecting the camera to the phone.
- Verify that video is enabled in Cisco Unified Communications Manager.
- Check the resolution of the transmitting endpoint. Cisco Unified IP Phone 8961, 9951, and 9971 does not display videos that use a resolution higher than VGA. If the other endpoint transmits at a resolution greater than VGA, such a transmission results in a black screen.
- Verify that packets are being received. Check the Rcvr Packets (would be zero in this case) in **Administrator Settings** > **Status** > **Call Statistics** > **Video** > **Video Statistics**.
- Ensure that the transmitting phone has the camera shutter completely open.

Phone display is wavy

Problem

The display appears to have rolling lines or a wavy pattern.

Cause

The phone might be interacting with certain types of older fluorescent lights in the building.

Solution

Move the phone away from the lights or replace the lights to resolve the problem.

Video Freezes

Problem

The video is frozen.

Cause

When the phone stops receiving video packets, the video display pauses and displays the last decoded video frame.

Solution

- Check whether the received packets count is incrementing or not, by navigating to **Administrator Settings** > **Status** > **Call Statistics** > **Video** > **Video statistics** > **Rcvr Packets statistics**.
- Put the call on hold and then resume the call to clear the issue.
- If the transmitting phone is also Cisco Unified IP Phone 8961 or 9951 or 9971, check the LED on top of the camera. If no light is illuminated (either green or red), then the remote camera might not be transmitting video.

Audio/video is not synchronized

Problem

Audio/Video synchronization is poor.

Solution

To resolve synchronization issues:

- Check whether RTCP is enabled in Cisco Unified Communications Manager.
- Check for a degraded network connection by navigating to **Administrator Settings** > **Status** > **Call Statistics** > **Video** > **Video Statistics** and checking the Avg Jitter and Max Jitter values.
- Place the call on hold and then resume the call to restore audio/video synchronization.

No audio

Problem

The recipient endpoint only sees a mute image.

Solution

If Auto Transmit Video is set to **Off**, the camera automatically transmits the mute image. The illuminated red LED on the top of the camera indicates that the video is muted. Set the Auto Transmit Video setting to **On** to restore video on the other side.

Video is too dark

Problem

Video that the camera transmits is too dark or the subject too dark in the video.

Solution

The lighting conditions within the field of view of the camera affect the brightness of the video.

- Adjust the View Area for your camera. Try moving the location of the camera and check whether the brightness improves.
- Adjust the camera brightness by navigating to **Accessories** > **Cisco Unified Video Camera** > **Brightness** and adjusting the brightness settings.

Poor quality or grainy video

Problem

The phone has poor video quality/grainy video.

Solution

When the resolution of the received video is grainy, the user may perceive that the video quality is poor. However, this does not cause video distortion or artifacts.

- Check the Cisco Unified Communications Manager bandwidth settings under Region settings.
- Check the Receiver Resolution in video statistics. This may be an issue if the Cisco Unified Communications Manager bandwidth setting limits the resolution to less than CIF, (352x288). Try increasing the bandwidth to at least 275 kbps.

Video is blocky or distorted

Problem

The phone has blocky or distorted video.

Cause

Blocky or distorted video is generally a symptom of a degraded network. Endpoints that do not closely adhere to video transmission standards can also cause blocky or distorted video.

Solution

If the network is degraded, navigate to **Administrator Settings** > **Status** > **CallStatistics** > **Video** > **Video Statistics** and check the following fields:

- Rcvr Lost Packets
- Rcvr Discarded
- Avg Jitter
- Max Jitter

Video is slow moving or jittery

Problem

The phone has slow moving video or jittery video.

Cause

The frame rate of the received video is low.

Solution

Check the rate by navigating to **Administrator Settings** > **Status** > **CallStatistics** > **Video** > **Video Statistics** and checking the Rcvr Frame Rate field. Frame rates of fewer than 15 fps result in slow-moving video.

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.

Poor Audio Quality with Calls That Route Outside Cisco Unified Communications Manager

Problem

Poor quality occurs with tandem audio encoding. Tandem encoding can occur when calls are made between an IP Phone and a digital cellular phone, when a conference bridge is used, or in situations where IP-to-IP calls are partially routed across the PSTN.

Cause

In these cases, use of voice codecs such as G.729 and iLBC may result in poor voice quality.

Solution

Use the G.729 and iLBC codecs only when absolutely necessary.

Video distorted or pixilated on Cisco Unified IP Phone 9951

Problem

The video on the Cisco Unified IP Phone 9951 appears distorted or pixilated and the phone is using a 100-BaseT/full duplex connection.

Cause

The transmission speed of the connection is insufficient for the audio and video demands of the phone.

Solution

Upgrade the transmission speed to 1000-BaseT/full duplex.

VXC VPN Troubleshooting

When you are experiencing problems associated with the Virtualization Experience Client (VXC) Virtual Private Network (VPN), use this section to troubleshoot the problems.

Phone Does Not Set Up VXC VPN Tunnel

Problem

The VXC is on and physically connected with phone using the spine connector and network cable, but the VXC VPN status is `not connected`.

Solution

Perform the following steps:

1. Verify that:
   a. The phone is powered by the adapter.
   b. VXC is shown in accessories menu. If not, power cycle the phone.
   c. VPN status is connected.
2. Power cycle VXC device.

Identify VXC VPN Connection Problems

Use these steps to identify problems with the VXC VPN connection.

Procedure

Step 1 Check that the VXC is showing in the phone Accessories menu.

Step 2 Check the VXC VPN status in the phone VPN menu.

Step 3 In the Cisco Unified Communications Manager, check that the Enable VXC VPN for MAC fields contains all Fs or is the same MAC address of the user's VXC device.

Step 4 Check that the VXC VPN status is connected.

Step 5 Check that the Alternate TFTP is enabled and that the correct TFTP IP address is configured on the phone.

Step 6 Check that the VXC is physically connected in the PC port of the phone.

Step 7 Check that the VXC device gets an IP address from the phone, and not from the local router.

Step 8 From the VXC device, use the *ping* command to check that the device can successfully contact the Cisco Unified Communications Manager.

General telephone call problems

The following sections help troubleshoot general telephone call problem.

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.

Check TFTP settings

Procedure

Step 1 You can determine the IP address of the TFTP server that the phone uses by pressing **Applications**, then selecting **Administrator Settings** > **Network Setup** > **Ethernet Setup** > **IPv4 Setup** > **TFTP Server 1**.

Step 2 If you have assigned a static IP address to the phone, you must manually enter a setting for the TFTP Server 1 option. For more information, see Ethernet Setup menu, on page 104.

Step 3 If you are using DHCP, the phone obtains the address for the TFTP server from the DHCP server. Check that the IP address is configured in Option 150.

Step 4 You can also enable the phone to use an alternate TFTP server. Such a setting is particularly useful if the phone recently moved from one location to another. See Ethernet Setup menu, on page 104 for instructions.

Step 5 If the local DHCP does not offer the correct TFTP address, enable the phone to use an alternate TFTP server. This is often necessary in VPN scenario.

Determine DNS or connectivity issues

Procedure

Step 1 Use the Reset Settings menu to reset phone settings to their default values. See Basic Reset, on page 290 for details.

Step 2 Modify DHCP and IP settings:

a) Disable DHCP. See Ethernet Setup menu, on page 104 for instructions.

b) Assign static IP values to the phone. See Ethernet Setup menu, on page 104 for instructions. Use the same default router setting that other functioning Cisco Unified IP Phones use.

c) Assign a TFTP server. See Ethernet Setup menu, on page 104 for instructions. Use the same TFTP server that other functioning Cisco Unified IP 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 Unified IP Phone. For information about determining a MAC address, see Cisco Unified IP Phone MAC Address Determination, on page 52.

Step 6 Power cycle the phone.

Check DHCP settings

Procedure

Step 1 On the Cisco Unified IP Phone, press **Applications**.

Step 2 Select **Administrator Settings** > **Network Setup** > **Ethernet Setup** > **IPv4 Setup**, and look at the following options:

- DHCP Server: If you have assigned a static IP address to the phone, you do not need to enter a value for the DHCP Server option. 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:

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

- IP Address, Subnet Mask, Default Router: If you have assigned a static IP address to the phone, you must manually enter settings for these options. See Ethernet Setup menu, on page 104 for instructions.

Step 3 If you are using DHCP, check the IP addresses that your DHCP server distributes.
See the *Understanding and Troubleshooting DHCP in Catalyst Switch or Enterprise Networks* document, available at this URL:

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

Create new phone configuration file

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. See the *Cisco Unified Communications Manager Administration Guide* for more information.
- 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.

To create a new configuration file, follow these steps:

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. See the *Cisco Unified Communications Manager Administration Guide* for more information.

Step 3 Add the phone back to the Cisco Unified Communications Manager database. See Cisco Unified Communications Manager Phone Addition Methods, on page 50 for details.

Step 4 Power cycle the phone.

Identify 802.1X authentication problems

Procedure

Step 1 Verify that you have properly configured the required components (see 802.1X Authentication, on page 33 for more information).

Step 2 Confirm that the shared secret is configured on the phone (see 802.1X Authentication and Transaction Status, on page 125 for more information).

- If the shared secret is configured, verify that you have the same shared secret on the authentication server.
- If the shared secret is not configured on the phone, enter it, and ensure that it matches the shared secret on the authentication server.

Verify DNS settings

To verify DNS settings, follow these steps:

Procedure

Step 1 Press **Applications**.

Step 2 Select **Administrator Settings** > **Network Setup** > **Ethernet Setup** > **IPv4 Setup** > **DNS Server 1**.

Step 3 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

Note A service must be activated before it can be started or stopped. To activate a service, choose **Tools** > **Service Activation**.

To start a service, follow these steps:

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.

Enable phone debugging

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.

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

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.

Contact Cisco TAC for more information and assistance.

Procedure

	Command or Action	Purpose
Step 1	In Cisco Unified Communications Manager Administration, navigate to one of the following windows:	• **Device** > **Device settings** > **Common Phone Profile** • **System** > **Enterprise Phone Configuration** • **Device** > **Phone**
Step 2	Select the phone to be debugged.	
Step 3	To turn debugging on, set the following parameters	• Log Profile - values: Preset (default), Default, Telephony • Remote Log - values: Disable (default), Enable • IPv6 Log Server or Log Server - IP address (IPv4 or address) IP addresses can include a port. The format for IPv6 Log Server or Log Server is [address]:<port>@@base=<0-7>;pfs=<0-1>. 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

	Command or Action	Purpose
		• 7 - Debugging
Step 4	Select **Save**.	
Step 5	On the phone, perform the functions.	
Step 6	Return to the Cisco Unified Communications Manager Administration window selected in Step 1, and turn debugging off.	

General Troubleshooting Information

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

Table 57: Cisco Unified IP Phone troubleshooting

Summary	Explanation
Connecting a Cisco Unified IP Phone to another Cisco Unified IP Phone	Cisco does not support connecting an IP phone to another IP Phone through the PC port. Each IP Phone should connect directly to a switch port. If phones are connected together in a line by using the PC port, the phones do not work.
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 voice VLAN may cause IP phones to reset, lose an active call, or be unable to initiate or answer a 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 careful if you decide to unplug the network connection of the phone and plug the cable into a desktop computer. **Caution** The network card in the computer cannot receive power through the network connection; if power comes through the connection, the network card can be destroyed. To protect a network card, wait 10 seconds or longer after unplugging the cable from the phone before plugging it into a computer. This delay gives the switch enough time to recognize that there is no longer a phone on the line and to stop providing power to the cable.
Changing the telephone configuration	By default, the network configuration options are locked to prevent users from making changes that could impact their network connectivity. You must unlock the network configuration options before you can configure them. See Password Protection, on page 103 for details.

Summary	Explanation
Codec mismatch between the phone and another device	The RxType and the TxType statistics show the codec that is used for a conversation between this Cisco Unified IP Phone and the other device. The values of these statistics should match. If they do not, verify that the other device can handle the codec conversation, or that a transcoder is in place to handle the service. See Display Call Statistics Screen, on page 240 for information about displaying these statistics.
Sound sample mismatch between the phone and another device	The RxSize and the TxSize statistics show the size of the voice packets that are used in a conversation between this Cisco Unified IP Phone and the other device. The values of these statistics should match. See Display Call Statistics Screen, on page 240 for information about displaying these statistics.
Loopback condition	A loopback condition can occur when the following conditions are met: • The SW Port Configuration option in the Network Configuration menu on the phone is set to 10 Half (10-BaseT/half 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 following message appears in the switch console log: HALF_DUX_COLLISION_EXCEED_THRESHOLD To resolve this problem, reenable the port from the switch.

Additional troubleshooting information

If you have additional questions about troubleshooting Cisco Unified IP Phones, go to the following Cisco website and navigate to the desired Cisco Unified IP Phone:

http://www.cisco.com/cisco/web/psa/troubleshoot.html

Maintenance

The following sections describe phone maintenance.

Basic Reset

Performing a reset of a Cisco Unified IP Phone provides a way to recover if the phone experiences an error and resets or restores various configuration and security settings.

The following sections describe the types of resets that you can perform. You can reset a phone with any of these operations after the phone has started up. Choose the operation that is appropriate for your situation.

Perform Factory Reset

Resets user and network configuration settings to their factory default values, and restarts the phone.

Before you perform a factory reset, ensure that the following conditions are met:

- The phone must be on a DHCP-enabled network.
- A valid TFTP server must be set in DHCP option 150 or option 66 on the DHCP server.

The following events occur on the phone when you perform a reset:

- User configuration settings reset to default values.
- Network configuration settings reset to default values.
- Call histories get erased.
- Locale information resets to default values.
- Phone application gets erased, and the phone recovers by using the image in the inactive partition of flash to boot up.
- Security settings reset to default values. This includes deleting the CTL file, deleting the MD5 secret, and changing the 802.1x Device Authentication parameter to “Disabled.”

Note Do not power down the phone until the factory reset process completes and the main screen appears.

Procedure

Step 1 From the Administrator Settings menu, unlock phone options (see Password Protection, on page 103).

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

Perform factory reset from phone keypad

Use these steps to reset the phone to factory default settings using the phone keypad.

Procedure

Step 1 While powering up the phone, press and hold #.

Step 2 When the light on the Mute button and handset light strip turns off and all other lights (Line button, Headset button, Speakerphone button and Select button) stay green, press **123456789*0#** in sequence.
When you press **1**, the lights on the line buttons turn red. The light on the Select button flashes when a button is pressed.

If you press the buttons out of sequence, the lights on the line button, headset button, speakerphone button, and Select button turn green. You need to start over and press **123456789*0#** in sequence again.

After you press these buttons, the phone goes through the factory reset process.

Caution Do not power down the phone until it completes the factory reset process, and the main screen appears.

Perform Network Configuration Reset

Resets network configuration settings to their default values and resets the phone. This method causes DHCP to reconfigure the IP address of the phone.

Procedure

Step 1 From the Administrator Settings menu, unlock phone options (see Password Protection, on page 103).

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

Perform user and network configuration reset

Resets any user and network configuration changes that you have made, but that the phone has not written to flash memory, to previously saved settings.

Procedure

Step 1 From the Administrator Settings menu, unlock phone options (see Password Protection, on page 103).

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

Remove CTL File

Deletes only the CTL file from the phone.

Procedure

Step 1 From the Administrator Settings menu, unlock phone options (seePassword Protection, on page 103).

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

Quality Report Tool

The Quality Report Tool (QRT) is a voice quality and general problem-reporting tool for the Cisco Unified IP Phone. The QRT feature is installed as part of Cisco Unified Communications Manager installation.

You can configure user Cisco Unified IP Phones with QRT. When you do so, users can report problems with phone calls by pressing Report Quality. This softkey or button is available only when the Cisco Unified IP Phone is in the Connected, Connected Conference, Connected Transfer, or OnHook states.

When a user presses Report Quality, a list of problem categories appears. The user selects the appropriate problem category, and this feedback is logged in an XML file. Actual information that is logged depends on the user selection and whether the destination device is a Cisco Unified IP Phone.

For more information about using QRT, see *Cisco Unified Communications Manager Features and Services Guide*.

Voice Quality Monitoring

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

- Concealment Ratio metrics 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 that are 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 Unified IP Phone by using the Call Statistics screen (see Display Call Statistics Screen, on page 240) or remotely by using Streaming Statistics (see Remote Monitoring, on page 247).

Voice Quality Troubleshooting Tips

When you observe significant and persistent changes to metrics, use the following table for general troubleshooting information:

Table 58: Changes to Voice Quality Metrics

Metric change	Condition
Conceal Ratio and Conceal Seconds increase significantly.	Network impairment from packet loss or high jitter.

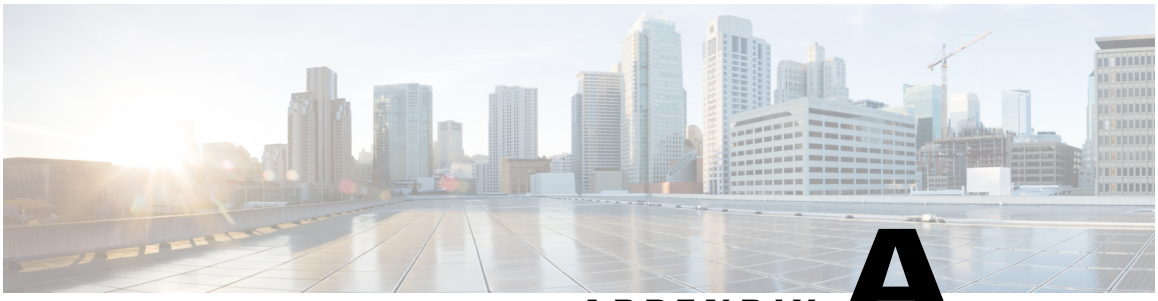
Metric change	Condition
Conceal Ratio is near or at zero, but the voice quality is poor.	• Noise or distortion in the audio channel such as echo or audio levels. • Tandem calls that undergo multiple encode/decode, such as calls to a cellular network or to a calling card network. • Acoustic problems that come 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.

Note Voice quality metrics do not account for noise or distortion; they account only for frame loss.

Cisco Unified IP Phone Cleaning

To clean your Cisco Unified 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 nonweatherproof electronics, liquids and powders can damage the components and cause failures.

When the phone is in sleep mode, the touchscreen 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. If the phone is likely to wake up during cleaning, wake it up or wait until it is awake before following the preceding cleaning instructions.



APPENDIX A

Internal Support Website

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

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

Consider including the following types of information on this site:

Cisco Unified IP Phone User Support

To successfully use some of the features on the Cisco Unified IP Phone (including Speed Dial, 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.

User Options Web Pages Access

Before a user can access the User Options web pages, you must use Cisco Unified Communications Manager Administration to add the user to a standard Cisco Unified Communications Manager End User group: choose **User Management** > **User Groups**. For more information, see:

- *Cisco Unified Communications Manager Administration Guide*, “User Group Configuration” chapter
- *Cisco Unified Communications Manager System Guide*, “Roles and User Groups” chapter

Phone Features User Subscription and Setup

End users can perform a variety of activities by using the Cisco Unified Communications Manager User Options web pages. These activities include subscribing to services, setting up speed dial and call forwarding numbers, configuring ring settings, and creating a personal address book. Keep in mind that configuring settings on a phone by using a website might be new for your end users. You need to provide as much information as possible to ensure that they can successfully access and use the User Options web pages.

Make sure to provide end users with the following information about the User Options web pages:

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

  http://<*server_name:portnumber*>/**ccmuser**/, where *server_name* is the host on which the web server is installed.

- A user ID and default password that are needed to access the application.

  These settings correspond to the values you entered when you added the user to Cisco Unified Communications Manager (see the Add Users to Cisco Unified Communications Manager, on page 181).

- A brief description of what a web-based, graphical user interface application is, and how to access it with a web browser.

- An overview of the tasks that users can accomplish by using the web page.

User Voice Messaging System Access

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

You should provide this information to each user:

- How to access the voice messaging system account.

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

- Initial password for accessing the voice messaging system.

  Make sure that you have configured a default voice messaging system password for all users.

- How the phone indicates that voice messages are waiting.

  Make sure that you have used Cisco Unified Communications Manager to set up a message waiting indicator (MWI) method.

User Personal Directory Entries Setup

Users can configure personal directory entries on the Cisco Unified IP Phone. To configure a personal directory, users must have access to the following:

- User Options web pages - Make sure that users know how to access their User Options web pages. See Phone Features User Subscription and Setup, on page 296 for details.
- Cisco Unified IP Phone Address Book Synchronizer - Make sure to provide users with the installer for this application:

Obtain Cisco Unified IP Phone Address Book Synchronizer

To download a copy of the synchronizer to send to your users, follow these steps:

Procedure

Step 1 To obtain the installer, choose **Application** > **Plugins** from Cisco Unified Communications Manager Administration.

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

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

Step 4 Send the TabSyncInstall.exe file and the instructions in Cisco Unified IP Phone Address Book Synchronizer Deployment, on page 297 to all users who require this application.

Cisco Unified IP Phone Address Book Synchronizer Deployment

The Cisco Unified IP Phone Address Book Synchronizer synchronizes data that is stored in your Microsoft Windows address book with the Cisco Unified Communications Manager directory and the User Options Personal Address Book.

Tip To successfully synchronize the Windows address book with the Personal Address Book, all Windows address book users should be entered in the Windows address book before you perform the following procedures.

Install Synchronizer

To install the Cisco Unified IP Phone Address Book Synchronizer, follow these steps:

Procedure

Step 1 Get the Cisco Unified IP Phone Address Book Synchronizer installer file from your system administrator.

Step 2 Double-click the TabSyncInstall.exe file that your administrator provided.
The publisher dialog box displays.

Step 3 Select **Run**.

The Welcome to the InstallShield Wizard for Cisco Unified CallManager Personal Address Book Synchronizer window displays.

Step 4 Select **Next**.
The License Agreement window displays.

Step 5 Read the license agreement information, and select the **I Accept**. Select **Next**.
The Destination Location window displays.

Step 6 Choose the directory in which you want to install the application and select **Next**.
The Ready to Install window displays.

Step 7 Select **Install**.
The installation wizard installs the application to your computer. When the installation is complete, the InstallShield Wizard Complete window displays.

Step 8 Select **Finish**.

Step 9 To complete the process, follow the steps in Set Up Synchronizer, on page 298.

Set Up Synchronizer

To configure the Cisco Unified IP Phone Address Book Synchronizer, perform these steps:

Procedure

Step 1 Open the Cisco Unified IP Phone Address Book Synchronizer.
If you accepted the default installation directory, you can open the application by choosing **Start** > **All Programs** > **Cisco Systems** > **TabSync**.

Step 2 To configure user information, select **User**.
The Cisco Unified CallManager User Information window displays.

Step 3 Enter the Cisco Unified IP Phone user name and password and select **OK**.

Step 4 To configure Cisco Unified Communications Manager server information, select **Server**.
The Configure Cisco Unified CallManager Server Information window displays.

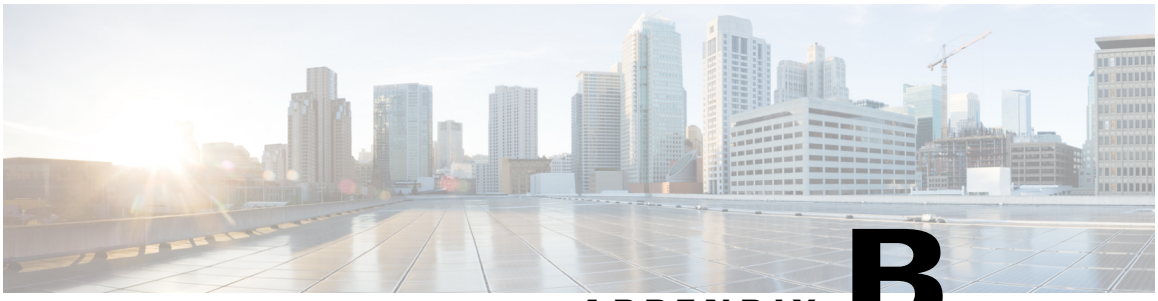
Step 5 Enter the IP address or host name and the port number of the Cisco Unified Communications Manager server and select **OK**.
If you do not have this information, contact your system administrator.

Step 6 To start the directory synchronization process, select **Synchronize**.
The Synchronization Status window provides the status of the address book synchronization. If you chose the user intervention for duplicate entries rule and you have duplicate address book entries, the Duplicate Selection window displays.

Step 7 Choose the entry that you want to include in your Personal Address Book and select **OK**.

Step 8 When synchronization is complete, select **Exit** to close the Cisco Unified CallManager Address Book Synchronizer.

Step 9 To verify whether the synchronization worked, sign in to your User Options web pages and choose **Personal Address Book**. The users from your Windows address book should be listed.



APPENDIX B

International User Support

Translated and localized versions of the Cisco Unified IP Phones are available in several languages. If you are supporting Cisco Unified IP Phones in a non-English environment, see the following sections to ensure that the phones are set up properly for your users:

- Cisco Unified Communications Manager Locale Installer Installation, page 301
- International Call Logging Support, page 301

Cisco Unified Communications Manager Locale Installer Installation

If you are using Cisco Unified IP Phones in a locale other than English (United States), you must install the locale-specific version of the Cisco Unified Communications Manager Locale Installer on every Cisco Unified Communications Manager server in the cluster. Installing the locale installer ensures that you have the latest translated text, user and network locales, and country-specific phone tones that are available for the Cisco Unified IP Phones. You can find locale-specific versions of the Cisco Unified Communications Manager Locale Installer at http://www.cisco.com/kobayashi/sw-center/telephony/callmgr/locale-installer.shtml.

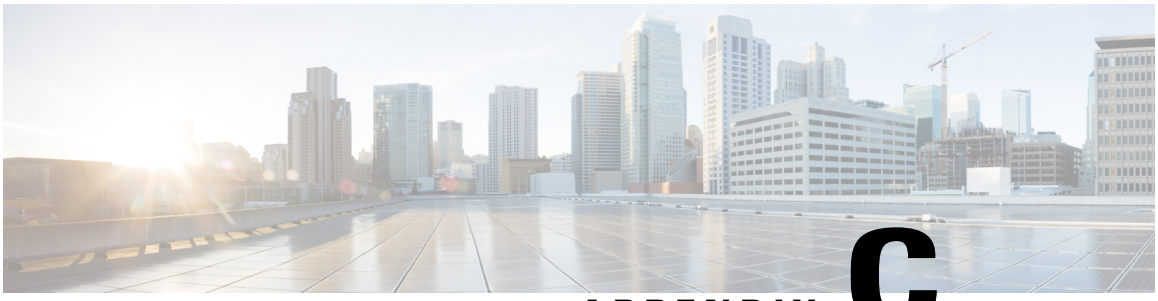
For more information, see the "Locale Installation" section in the *Cisco Unified Communications Operating System Administration Guide*.

Note All languages may not be immediately available, so continue to check the website for updates.

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.



APPENDIX C

Technical Specifications

The following sections describe the technical specifications for the Cisco Unified IP Phone 8961, 9951, and 9971.

Physical and Operating Environment Specifications

The following table shows the physical and operating environment specifications for the Cisco Unified IP Phone 8961, 9951, and 9971.

Table 59: Physical and Operating Specifications

Specification	Value or range
Operating temperature	32° to 104°F (0° to 40°C)
Operating relative humidity	10% to 95% (noncondensing)
Storage temperature	14° to 140°F (–10° to 60°C)
Height	8 in. (20.32 cm)
Width	10.5 in. (26.67 cm)
Depth	6 in. (15.24 cm)
Weight	3.5 lb. (1.6 kg)
Power	100-240 VAC, 50-60 Hz, 0.5 A when using the AC adapter 48 VDC, 0.2 A when using the in-line power over the network cable

Specification	Value or range
Power consumed by the camera (Applicable to Cisco Unified IP Phone 9951 and 9971)	290mA (1.45W) (excludes the power consumed by the phone)
Cables	Category 3/5/5e/6 for 10-Mbps cables with 4 pairs Category 5/5e/6 for 100-Mbps cables with 4 pairs Category 5e/6 for 1000-Mbps cables with 4 pairs **Note** Cables have 4 pairs of wires for a total of 8 conductors.
Distance requirements	As supported by the Ethernet Specification, the maximum cable length between each Cisco Unified IP Phone and the switch is assumed to be 330 feet (100 meters).

Note For power information regarding the Cisco Unified IP Key Color Expansion Module, see KEM Power Information, on page 72.

Cable Specifications

The following information lists the cable specifications:

- RJ-9 jack (4-conductor) for handset and headset connection
- RJ-45 jack for the LAN 10/100/1000BaseT connection (10/100/1000 Network port on the Cisco Unified IP Phone 8961, 9951, and 9971)
- RJ-45 jack for a second 10/100/1000BaseT compliant connection (10/100/1000 Computer port on the Cisco Unified IP Phone 8961, 9951, and 9971)
- 3.5 mm jack for microphone and speaker connection (for Cisco Unified IP Phone 9951 and 9971 only)
- 48-volt power connector

Network and Computer Port Pinouts

Although both the network and computer (access) ports are used for network connectivity, they serve different purposes and have different port pinouts.

- The network port is the 10/100/1000 SW port on the Cisco Unified IP Phone.
- The computer (access) port is the 10/100/1000 PC port on the Cisco Unified IP Phone.

Network Port Connector

The following table describes the network port connector pinouts.

Table 60: Network Port Connector Pinouts

Pin number	Function
1	BI_DA+
2	BI_DA-
3	BI_DB+
4	BI_DC+
5	BI_DC-
6	BI_DB-
7	BI_DD+
8	BI_DD-
Note BI stands for bidirectional, while DA, DB, DC and DD stand for Data A, Data B, Data C and Data D respectively.	

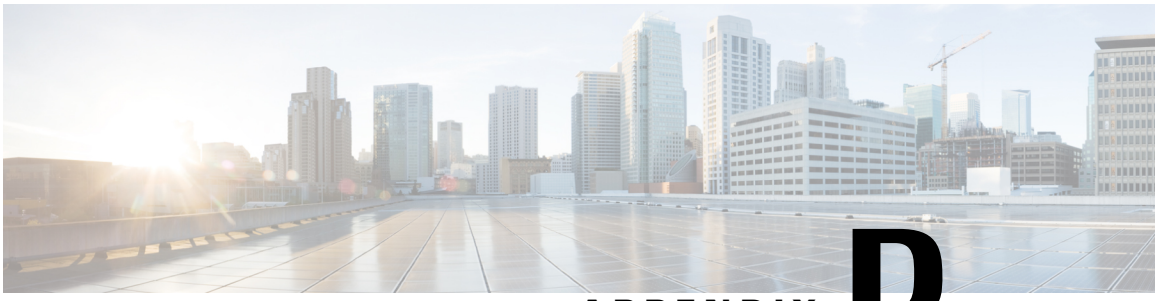
Computer Port Connector

The following table describes the computer port connector pinouts.

Table 61: Computer (Access) Port Connector Pinouts

Pin number	Function
1	BI_DB+
2	BI_DB-
3	BI_DA+
4	BI_DD+
5	BI_DD-
6	BI_DA-
7	BI_DC+

Pin number	Function
8	BI_DC-
Note BI stands for bidirectional, while DA, DB, DC and DD stand for Data A, Data B, Data C and Data D respectively.	



APPENDIX D

Basic Phone Administration Steps

This appendix provides minimum, basic configuration steps for you to do the following:

- Add a new user to Cisco Unified Communications Manager Administration
- Configure a new phone for that user
- Associate that user to that phone
- Complete other basic end user configuration tasks

The procedures provide one method for performing these tasks and are not the only way to perform the tasks. The procedures provide a streamlined approach to get a new user and corresponding phone running on the system.

These procedures are designed to be used on a mature Cisco Unified Communications Manager system where calling search spaces, partitions, and other complicated configuration are already done and are in place for existing users.

This section contains these topics:

Example user information

In the procedures that follow, examples are given when possible to illustrate some of the steps. Example user and phone information used throughout these procedures includes:

- User's Name: John Doe
- User ID: johndoe
- MAC address listed on phone: 00127F576611
- Five-digit internal telephone number: 26640

Cisco Unified Communications Manager User Addition

This section provides steps for adding a user to Cisco Unified Communications Manager. Follow one of the procedures in this section, depending on your operating system and the manner in which you are adding the user.

Add User from External LDAP Directory

If you added a user to an LDAP Directory (a non-Cisco Unified Communications Server directory), you can immediately synchronize that directory to the Cisco Unified Communications Manager on which you are adding this same user and the user phone by following these steps:

Procedure

Step 1 Sign into Cisco Unified Communications Manager Administration.

Step 2 Choose **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**.

Note If you do not need to 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. However, the synchronization must occur before you can associate a new user to a device.

Step 6 Proceed to Phone Setup, on page 309.

Add User Directly to Cisco Unified Communications Manager

If you are not using an 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 Choose **User Management** > **End User**, then click **Add New**. The End User Configuration window appears.

Step 2 In the User Information pane of this window, 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 3 Click **Save**.

Step 4 Proceed to Phone Setup, on page 309.

Phone Setup

To configure the phone, you must first identify the phone and then configure it by using the following procedures.

Identify phone

To identify the user phone model and protocol, follow these steps:

Procedure

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

Step 2 Select **Add New**.

Step 3 Select the user phone model from the Phone Type drop-down list, and select **Next**.
The Phone Configuration window appears. On the Phone Configuration window, you can use the default values for most of the fields.

Set up Phone Fields

To configure the required fields and some key additional fields, follow these steps:

Procedure

Step 1 For the required fields, possible values (some of which are based on the example of user johndoe) can be configured as follows:

a) In the Device Information pane of this window:

- MAC Address: Enter the MAC address of the phone, which is listed on a sticker that is affixed to the phone. Make sure that the value comprises 12 hexadecimal characters. Example: 00127F576611 (MAC address on john doe's phone)
- Description: Enter a useful description, such as john doe's phone, into this optional field. This helps you if you need to search on information about this user.
- Device Pool: Choose the device pool to which you want to assign this phone. The device pool defines sets of common characteristics for devices, such as region, date/time group, softkey template, and MLPP information.

  Note Device Pools are defined in the Device Pool Configuration window of Cisco Unified Communications Server Administration (**System** > **Device Pool**).

- Phone Button Template: Choose the appropriate phone button template from the drop-down list. The phone button template determines the configuration of buttons on a phone and identifies which feature (line, speed dial, and so on) corresponds to each button.

  Note Phone button templates are defined in the Phone Button Template Configuration window of Cisco Unified Communications Manager Administration (**Device** > **Device Settings** > **Phone Button Template**). You can use the search fields in conjunction with **Find** to find all configured phone button templates and their current settings.

- Common Phone Profile: From the drop-down lists, choose a common phone profile from the list of available common phone profiles.

  Note Common Phone Profiles are defined in the Common Phone Profile Configuration window of Cisco Unified Communications Manager Administration (**Device** > **Device Settings** > **Common Phone Profile**). You can use the search fields in conjunction with **Find** to find all configured common phone profiles and their current settings.

- Calling Search Space: From the drop-down lists, choose the appropriate calling search space (CSS). A calling search space comprises a collection of partitions (analogous to a collection of available phone books) that are searched to determine how a dialed number should be routed. The calling search space for the device and the calling search space for the directory number get used together. The directory number CSS takes precedence over the device CSS.

  Note Calling Search Spaces are defined in the Calling Search Space Configuration window of Cisco Unified Communications Manager Administration (**Calling Routing** > **Class of Control** > **Calling Search Space**). You can use the search fields in conjunction with **Find** to find all configured Calling Search Spaces and their current settings.

- Location: Choose the appropriate location for this Cisco Unified IP Phone.
- Owner User ID: From the drop-down lists, choose the user ID of the assigned phone user.

b) In the Protocol Specific Information area of this window, choose a Device Security Profile from the drop-down list. To enable security features for a phone, you must configure a new security profile for the device type and protocol and apply the security profile to the phone. If the phone does not support security, choose a nonsecure profile.
To identify the settings that the security profile contains, choose **System** > **Security Profile** > **Phone Security Profile**.

Note Choose a security profile based on the overall security strategy of the company.

c) In the Extension Information area of this window, check the Enable Extension Mobility check box if this phone supports Cisco Extension Mobility.
d) Click **Save**.

Step 2 Configure line settings:

a) In the Phone Configuration window, click Line 1 on the left pane of the window. The Directory Number Configuration window appears.
b) 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.

Example: 26640 is the directory number of user John Doe in the preceding example.

c) 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.
d) From the Calling Search Space drop-down list (Directory Number Settings area of the Directory Number Configuration window), choose the appropriate calling search space. A calling search space comprises a collection of partitions that are searched for numbers that are called from this directory number. The value that you choose applies to all devices that are using this directory number.
e) In the Call Pickup and Call Forward Settings area of the Directory Number Configuration window, 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.
f) In the "Line 1 on Device..." pane of the Directory Number Configuration window, configure the following:

- 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. You can also 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: Using the john doe extension in the preceding example, if you specify a mask of 408902XXXX, an external call from extension 6640 displays a caller ID number of 4089026640.

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

g) Click **Save**.
h) Click **Associate End Users** at the bottom of the window to associate a user to the line that is being configured. Use **Find** in conjunction with the Search fields to locate the user, then check the box next to the user name, then click **Add Selected**. The user name and user ID should now appear in the "Users Associated With Line" pane of the Directory Number Configuration window.
i) Click **Save**. The user is now associated with Line 1 on the phone.
j) If your phone has a second line, configure Line 2.
k) Associate the user with the device:

- Choose **User Management > End User**.

- Use the search boxes and Find to locate the user you have added (for example, doe for the last name).
- Click on the user ID (for example, johndoe). The End User Configuration window appears.
- Click **Device Associations**.
- Use the Search fields and **Find** to locate the device that you want to associate to the user. Select the device, then click **Save Selected/Changes**. The user is now associated with the device.
- Click **Go** next to the "Back to User" Related link in the upper right corner of the screen.

Step 3 Proceed to Perform final end user configuration steps, on page 312.

Perform final end user configuration steps

If you are not already jn the End User Configuration window, choose **User Management** > **End User** to perform some final configuration tasks. Use the Search fields and **Find** to locate the user (for example, John Doe), then click on the user ID to get to the End User Configuration window for the user.

In the End User Configuration window, follow these steps:

Procedure

Step 1 In the Directory Number Associations area of the screen, set the primary extension from the drop-down list.

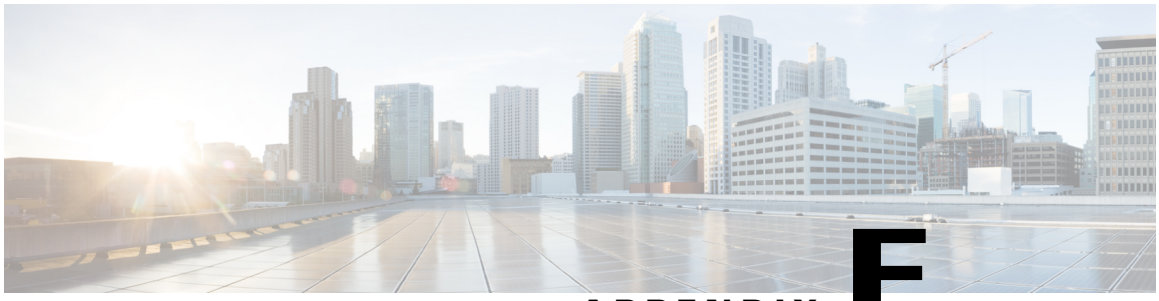
Step 2 In the Mobility Information area, check the Enable Mobility box.

Step 3 In the Permissions Information area, use the User 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.

Step 4 To view all configured user groups, choose **User Management** > **User Group**.

Step 5 In the Extension Mobility area, check the Enable Extension Mobility Cross Cluster box if the user is allowed for Extension Mobility Cross Cluster service.

Step 6 Select **Save**.



APPENDIX E

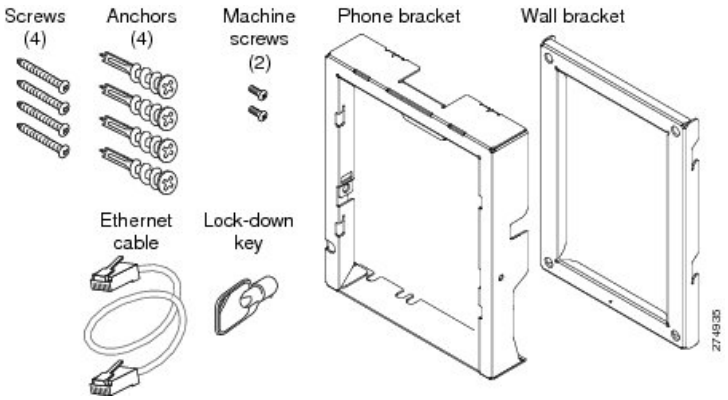
Cisco Unified IP Phone Wall Mount

This appendix contains information about installing the wall mount:

Wall Mount Components

This section describes how to install a wall mount for the Cisco Unified IP Phone 8961, 9951, and 9971.

Figure 5: Wall Mount Kit for a Single Phone Assembly



The package includes these items:

- One phone bracket
- One wall bracket
- Four #10-12x1-inch Phillips-head screws with 4 anchors
- One sheet metal screw (not shown)

- Two #4-40x1/4-inch machine screws
- One 6-inch Ethernet cable
- One key if the bracket includes the optional lock

Before You Begin

You need these tools to install the bracket:

- #1 and #2 Phillips-head screwdrivers
- Level

You must also install an Ethernet jack for the telephone in the desired location if an Ethernet jack does not currently exist. This jack must be wired appropriately for an Ethernet connection. You cannot use a regular telephone jack. For more information about phone installation requirements and warnings, see Cisco Unified IP Phone Installation, on page 55.

Install Bracket

To install the phone on the wall:

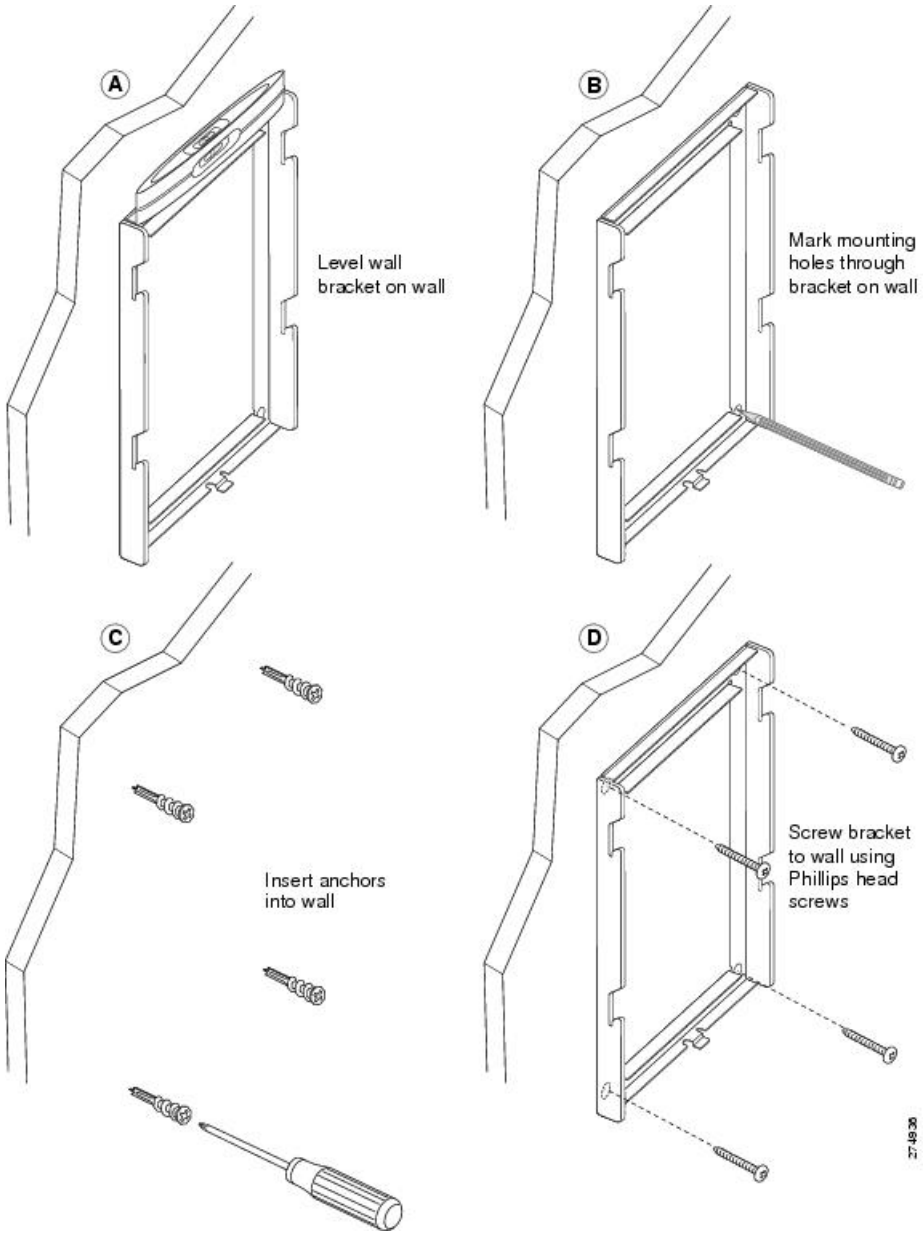
Procedure

Step 1 Mount the wall bracket in the desired location. You can install the bracket over an Ethernet jack, or you can run the Ethernet network cable to a nearby jack.

a) Use the level to ensure that the bracket is level, then use a pencil to mark the screw holes.
b) Using a #2 Phillips-head screwdriver, carefully center the anchor over the pencil mark and press the anchor into the wall.
c) Screw the anchor clockwise into the wall until it is seated flush.

d) Use the included screws and a #2 Phillips-head screwdriver to attach the bracket to the wall.

Figure 6: Mount the Wall Bracket



Step 2 Attach the phone bracket to the IP Phone.

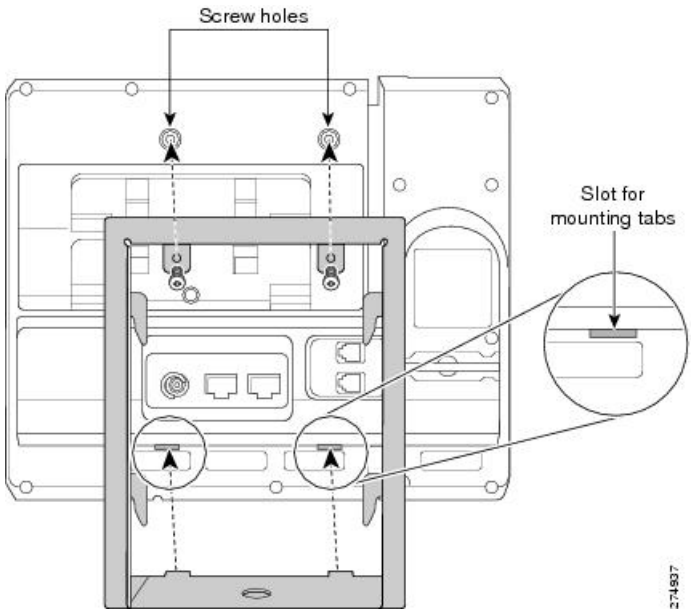
a) Detach the handset cord (and headset cord, if there is a headset), power cord, and any other attached cords from the base of the phone.

b) Remove the label covers that conceal the screw holes.

c) Attach the phone bracket by inserting the tabs into the mounting tabs on the phone. The phone ports should be accessible through the holes in the bracket.

d) Secure the phone bracket to the IP phone with the machine screws.
e) Thread the handset cord (and headset cord, if using one). Reattach the cords and seat them in the clips that are incorporated into the phone body.

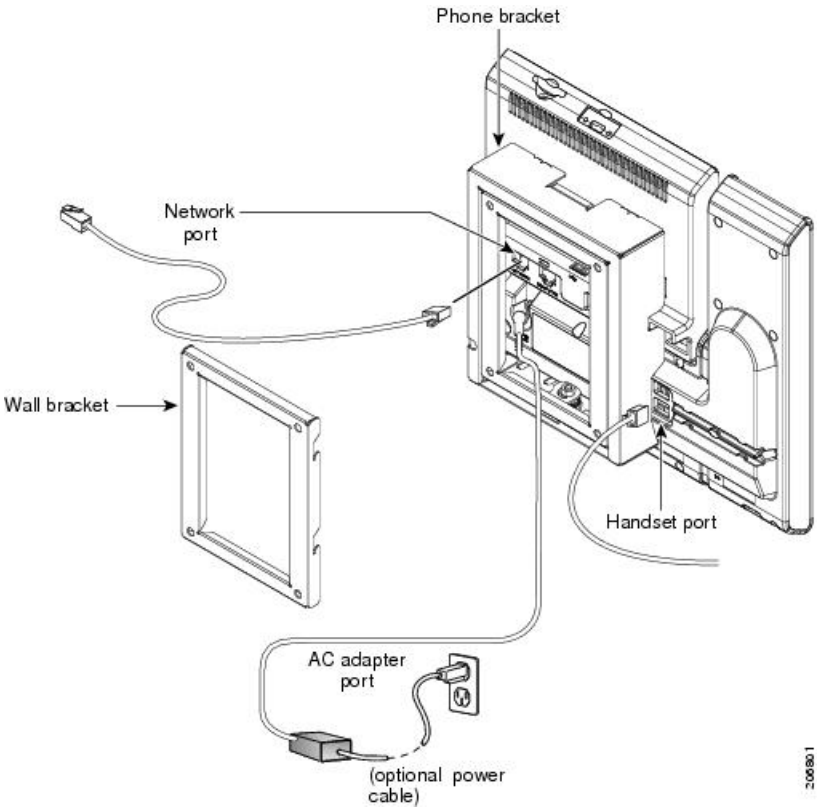
Figure 7: Attach the Phone Bracket



Step 3 Attach the Ethernet cable to the 10/100/1000 SW network port and wall jack.
If you are connecting a network device (such as a computer) to the phone, attach the cable to the 10/100/1000 Computer (PC access) port.

If you are using an external power supply, plug the power cord into the phone and dress the cord by clipping it into the clips that are incorporated into the phone body next to the PC port.

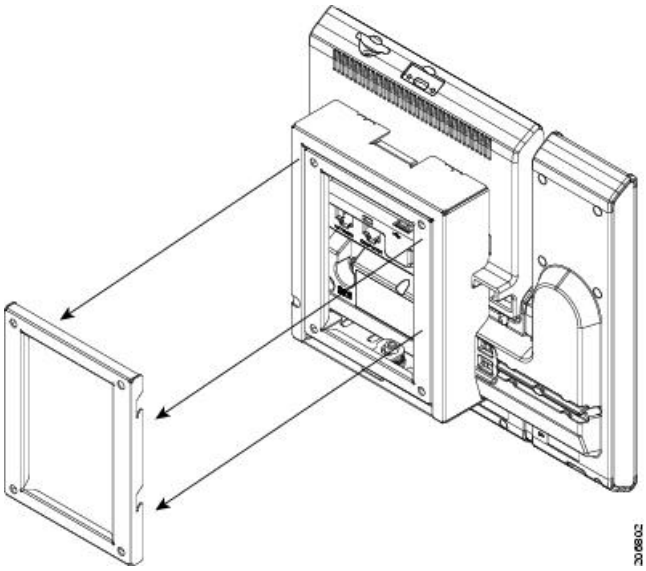
Figure 8: Attach the Cables



Step 4 Attach the phone to the wall bracket by inserting the tabs on the top of the phone bracket into the slots on the wall bracket. Ensure that the power cord and any other cable that does not terminate in the wall behind the

bracket are positioned in one of the cable-access openings in the bottom of the bracket. The phone and wall bracket openings together form circular openings with room for one cable per opening.

Figure 9: Attach the Phone to the Wall Bracket



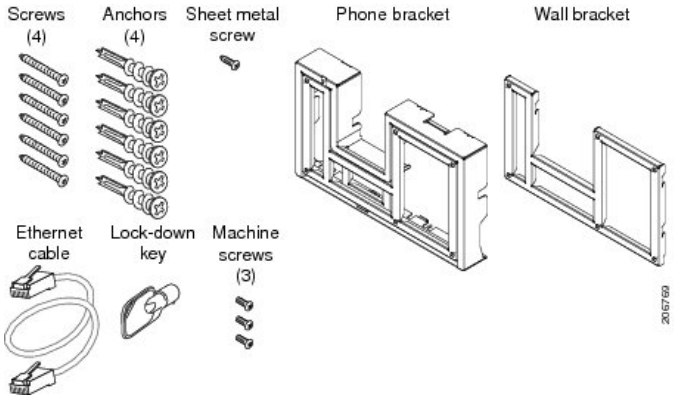
Step 5 Use the locking key to lock the phone to the wall bracket.

Step 6 Proceed to Adjust Handset Rest, on page 324.

Wall Mount Components for Phone with Key Expansion Module

This section describes how to install a wall mount for the Cisco Unified IP Phone 8961, 9951, and 9971 that connects to the Key Expansion Module.

Figure 10: Wall Mount Kit for Phone with Key Expansion Module



The package includes these items:

- One phone bracket
- One wall bracket
- Four #10-12x1-inch Phillips-head screws with 4 anchors
- One sheet metal screw
- Three #4-40x1/4-inch machine screws
- One 6-inch Ethernet cable
- One key if the bracket includes the optional lock

Before You Begin

You need these tools to install the bracket:

- #1 and #2 Phillips-head screwdrivers
- Level

You must also install an Ethernet jack for the telephone in the desired location if an Ethernet jack does not currently exist. This jack must be wired appropriately for an Ethernet connection. You cannot use a regular telephone jack. For more information about phone installation requirements and warnings, see Cisco Unified IP Phone Installation, on page 55.

Install Bracket for Phone with KEM

To install the phone on the wall, follow these steps:

Note Be sure to connect to connect the Cisco Unified IP Phone to the Key Expansion Module before installing the phone bracket.

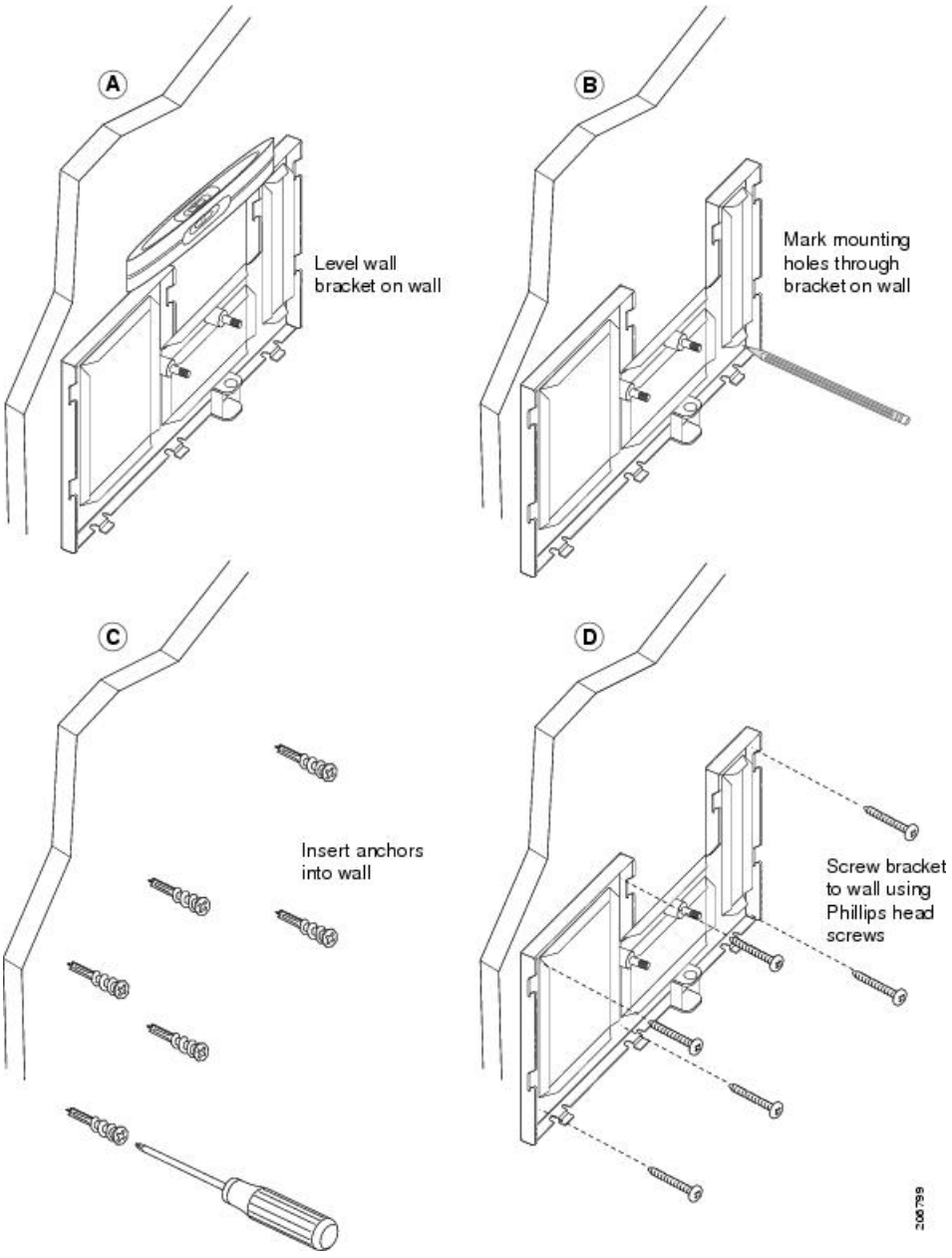
Procedure

Step 1 Mount the wall bracket in the desired location. You can install the bracket over an Ethernet jack, or you can run the Ethernet network cable to a nearby jack.

a) Use a level to ensure the bracket is level, then use a pencil to mark the screw holes.
b) Using a #2 Phillips-head screwdriver, carefully center the anchor over the pencil mark and press the anchor into the wall.
c) Screw the anchor clockwise into the wall until it is seated flush.

d) Use the included screws and a #2 Phillips-head screwdriver to attach the bracket to the wall.

Figure 11: Mount the Wall Bracket



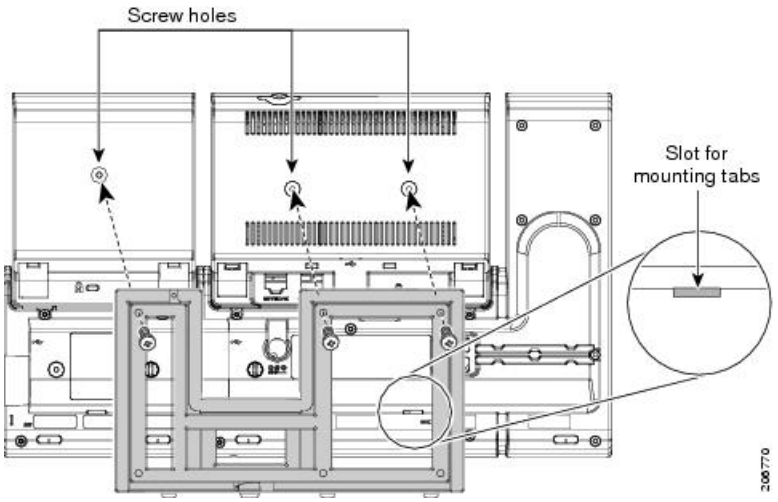
Step 2 Attach the phone bracket to the IP phone and key expansion assembly.

a) Detach the handset cord (and headset cord, if there is a headset), power cord, and any other attached cords from the base of the phone.

b) Remove the label covers that are conceal the screw holes.

c) Attach the phone bracket by inserting the tabs into the mounting tabs on the phone. The phone ports should be accessible through the holes in the bracket.
d) Secure the phone bracket to the IP phone with the machine screws.
e) Thread the handset cord (and headset cord, if using one). Reattach the cords and seat them in the clips that are incorporated into the phone body.

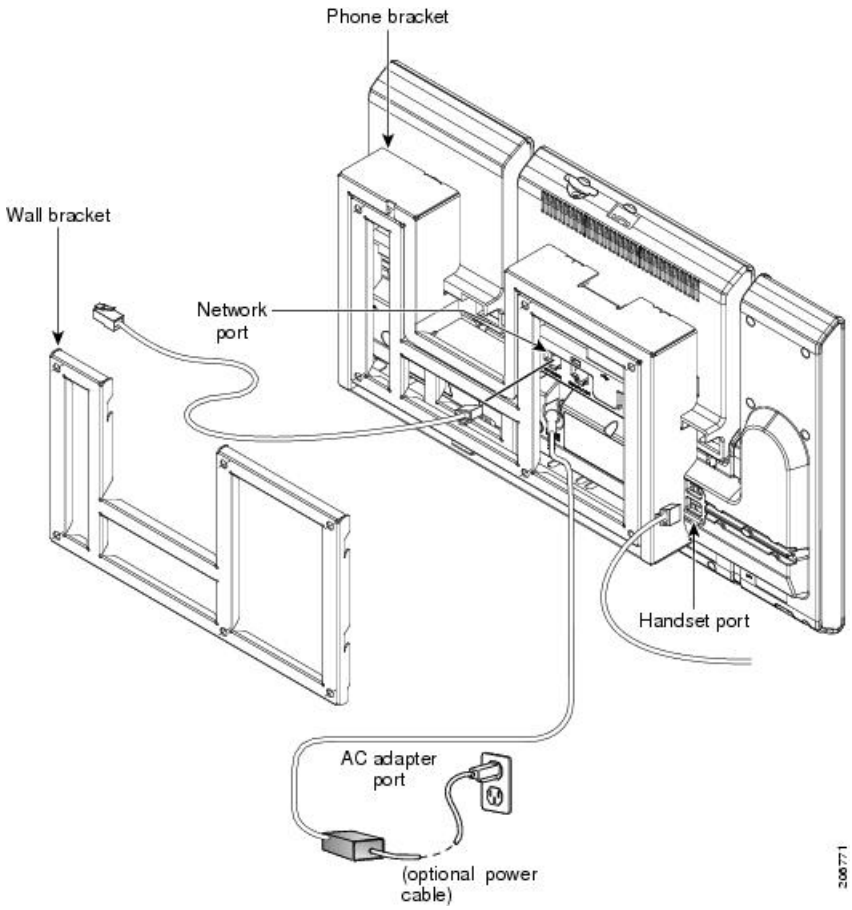
Figure 12: Attach the Phone Bracket



Step 3 Attach the Ethernet cable to the 10/100/1000 SW network port and wall jack.
If you are connecting a network device (such as a computer) to the phone, attach the cable to the 10/100/1000 Computer (PC access) port.

If you are using an external power supply, plug the power cord into the phone and dress the cord by clipping it into the clips that are incorporated into the phone body next to the PC port.

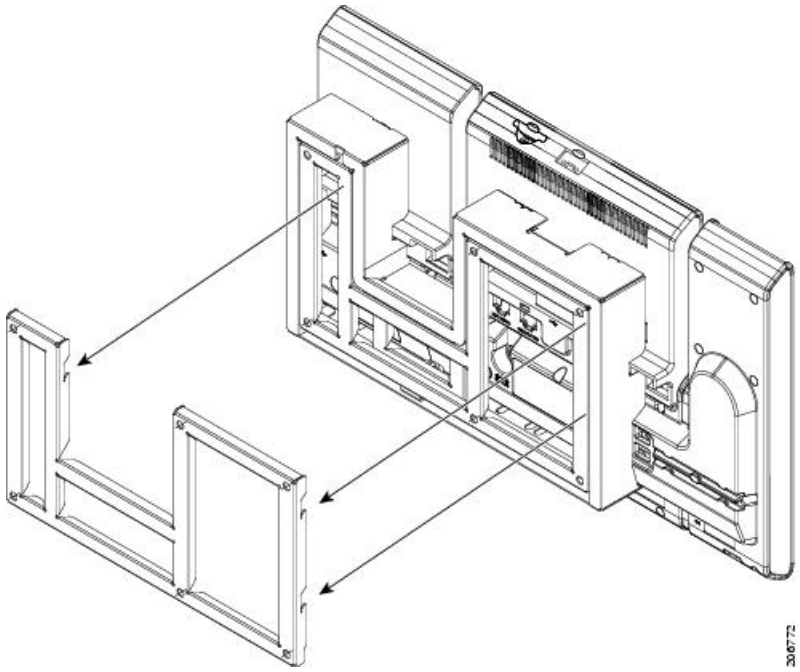
Figure 13: Attach the Cables



Step 4 Attach the phone to the wall bracket by inserting the tabs on the top of the phone bracket into the slots on the wall bracket.

Ensure that the power cord and any other cable that does not terminate in the wall behind the bracket are positioned in one of the cable-access openings in the bottom of the bracket. The phone and wall bracket openings together form circular openings with room for one cable per opening.

Figure 14: Attach the Phone to the Wall Bracket



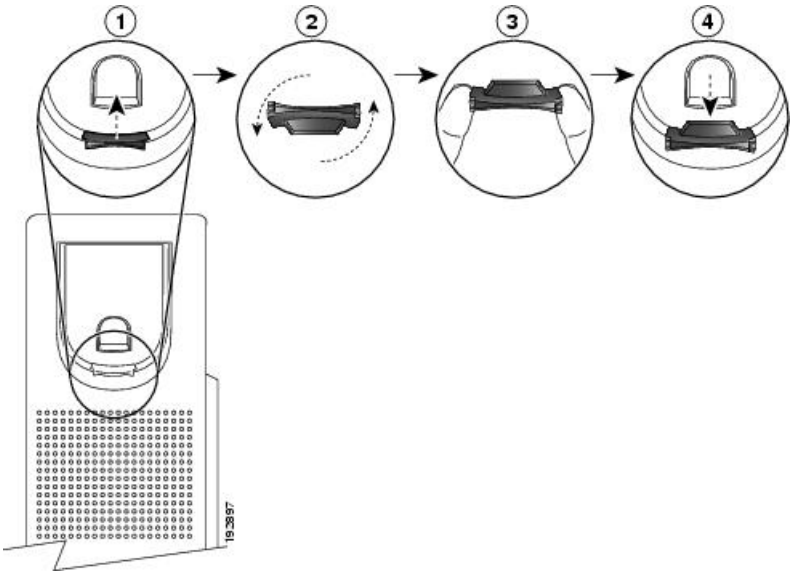
Step 5 Use the locking key to lock the phone to the wall bracket.

Step 6 Proceed to Adjust Handset Rest, on page 324

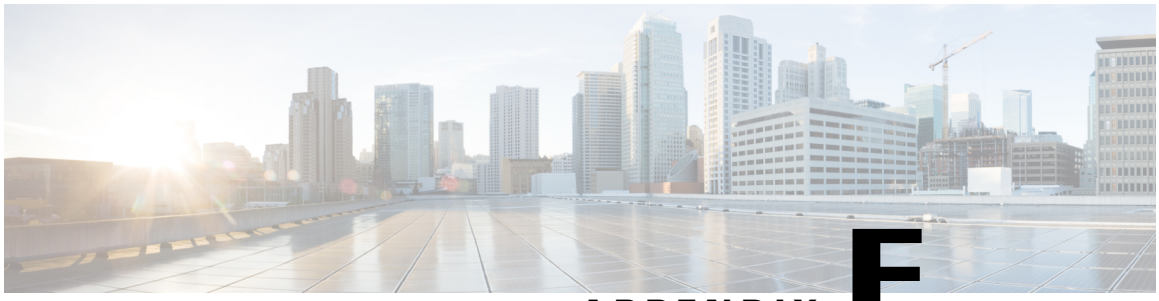
Adjust Handset Rest

With a wall-mounted phone, you might need to adjust the handset rest to ensure that the receiver does not slip out of the cradle. The hook should have a lip on which the handset catches when the phone is vertical. Follow the diagram and steps below to change the hookswitch hook.

Figure 15: Adjust the Handset Hook



1	Remove the handset from the cradle and pull the plastic tab from the handset rest.
2	Rotate the tab 180 degrees.
3	Hold the tab between two fingers, with the corner notches facing you.
4	Line up the tab with the slot in the cradle, and press the tab evenly into the slot. An extension protrudes from the top of the rotated tab. Return the handset to the handset rest.



APPENDIX F

Cisco Unified IP Phone Non-Lockable Wall Mount

This appendix contains the information for installing the following products:

- ADA Non-Lockable Wall Mount Kit for 8961 Series and 9900 Series IP Phones: Installed on the Cisco Unified IP Phone 8961, 9951, and 9971.
- ADA Non-Lockable Wall Mount Kit for 8961 Series and 9900 Series IP Phones plus a single Key Expansion Module: Installed on the Cisco Unified IP Phone 8961, 9951, and 9971 with the Key Expansion Module.

These nonlocking wall mount kits meet ADA 4.4.1 requirements.

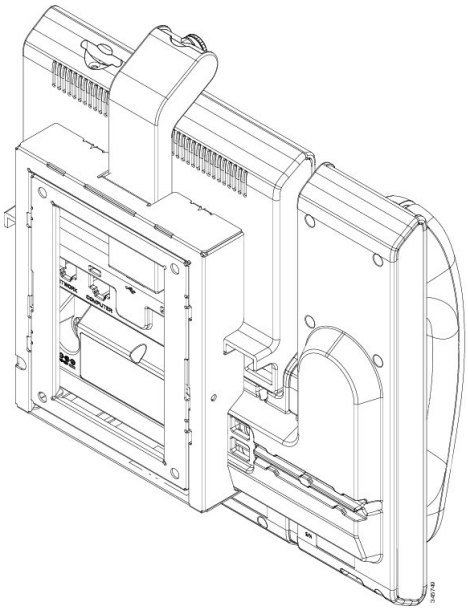
- ADA Non-Lockable Wall Mount Kit for 8961 Series and 9900 Series IP Phones, page 325
- ADA Non-Lockable Wall Mount Kit for 8961 Series and 9900 Series IP Phones with Key Expansion Module, page 334

ADA Non-Lockable Wall Mount Kit for 8961 Series and 9900 Series IP Phones

This section describes how to install the non-lockable wall mount kit on a Cisco Unified IP Phone 8961, 9951, and 9971 when the phone is not connected to a Key Expansion Module.

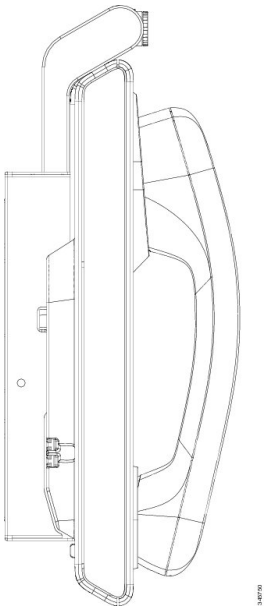
The following figure shows the wall mount kit installed on the phone.

Figure 16: Back View of ADA Non-Lockable Wall Mount Kit Installed on Phone



The following figure shows the phone with the wall mount kit from the side.

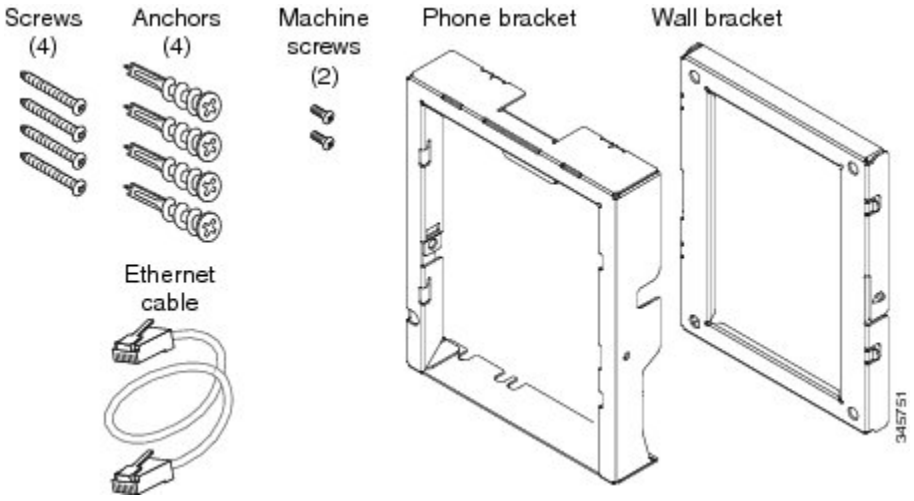
Figure 17: Side View of ADA Non-Lockable Wall Mount Kit Installed on Phone



Components

The following figure shows the components of the ADA Non-Lockable Wall Mount Kit for 8961 Series and 9900 Series IP Phones.

Figure 18: Components



The package contains the following items:

- One phone bracket
- One wall bracket
- Four #8-18 x 1.25-inch Phillips-head screws with four anchors
- Two #4-40 x 0.31-inch machine screws
- One 6-inch Ethernet cable

Before You Begin

You need these tools to install the bracket:

- #1 and #2 Phillips-head screwdrivers
- Level
- Pencil

You must also install an Ethernet jack for the telephone in the desired location if an Ethernet jack does not currently exist. This jack must be wired appropriately for an Ethernet connection. You cannot use a regular telephone jack. For more information about phone installation requirements and warnings, see Cisco Unified IP Phone Installation, on page 38.

Install Non-Lockable Wall Mount Kit for Phone

The wall mount kit can be mounted on most surfaces, including concrete, brick, and similar hard surfaces. To mount the kit on concrete, brick, or similar hard surfaces, you must provide the appropriate screws and anchors for your wall surface.

Procedure

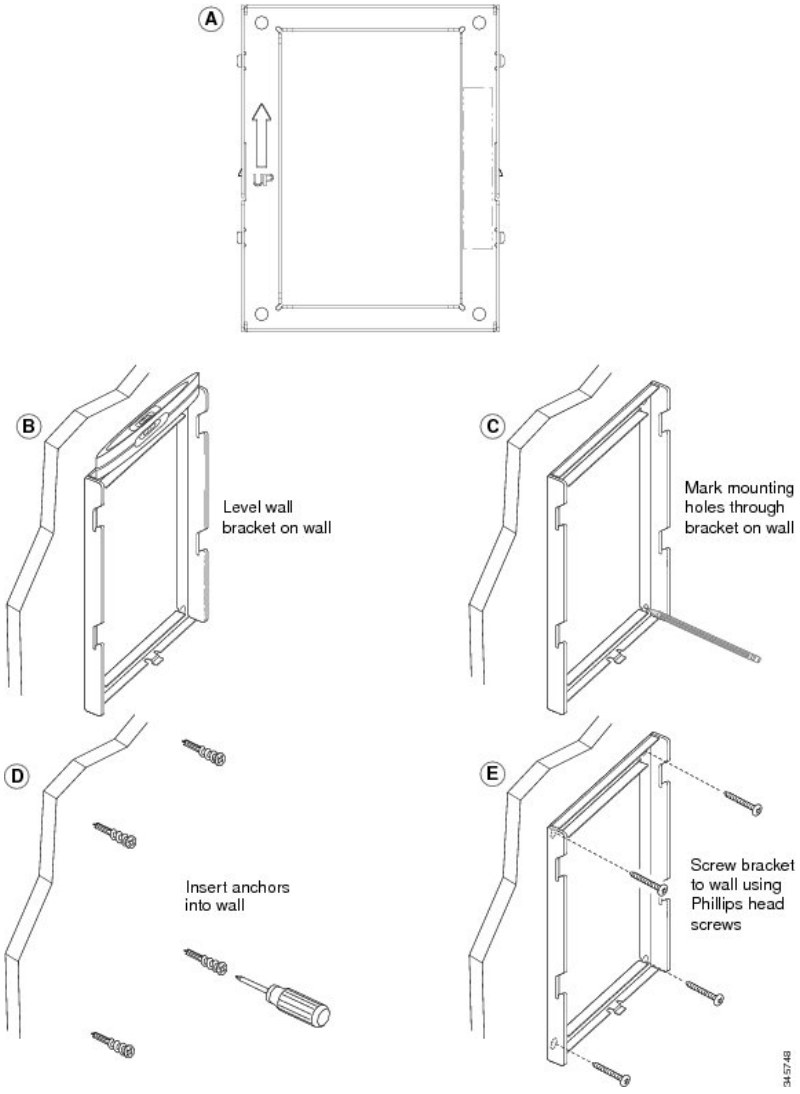
Step 1 Mount the wall bracket in the desired location. You can install the bracket over an Ethernet jack, or you can run the Ethernet network cable to a nearby jack.

Note If the jack is to be placed behind the phone, the Ethernet jack must be flush to the wall or recessed.

a) Hold the bracket on the wall, placing it so that the arrow on the back of the bracket is pointing up.
b) Use the level to ensure that the bracket is level and use a pencil to mark the screw holes.
c) Using a #2 Phillips-head screwdriver, carefully center the anchor over the pencil mark and press the anchor into the wall.
d) Screw the anchor clockwise into the wall until it is seated flush.
e) Use the included screws and a #2 Phillips-head screwdriver to attach the bracket to the wall.

The following figure shows the bracket installation steps.

Figure 19: Bracket Installation

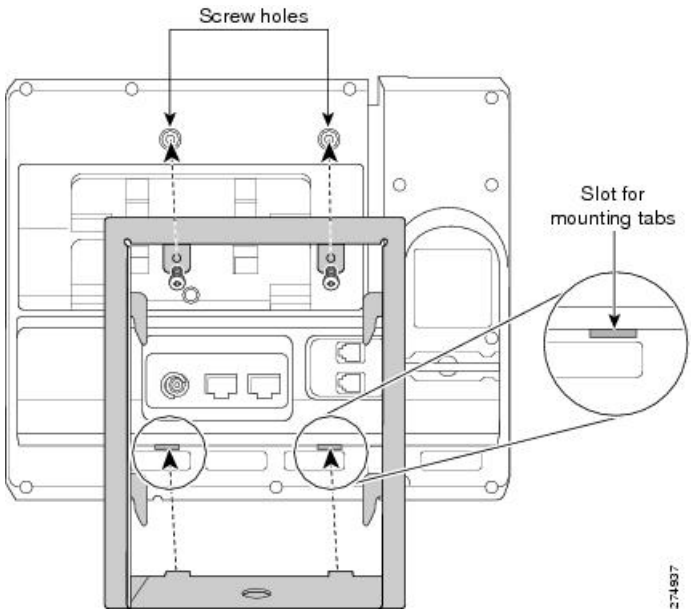


Step 2 Attach the phone bracket to the IP Phone.

a) Detach the handset cord (and headset cord, if there is a headset), power cord, and any other attached cords from the base of the phone.
b) Remove the label covers that conceal the screw holes.
c) Attach the phone bracket by inserting the tabs into the mounting tabs on the back of the phone. The phone ports should be accessible through the holes in the bracket.
d) Secure the phone bracket to the IP phone with the machine screws, using the #1 Phillips-head screwdriver.
e) Thread the handset cord (and headset cord, if using one). Reattach the cords and seat them in the clips that are incorporated into the phone body.

The following figure shows how the bracket attaches to the phone.

Figure 20: Attach Phone Bracket

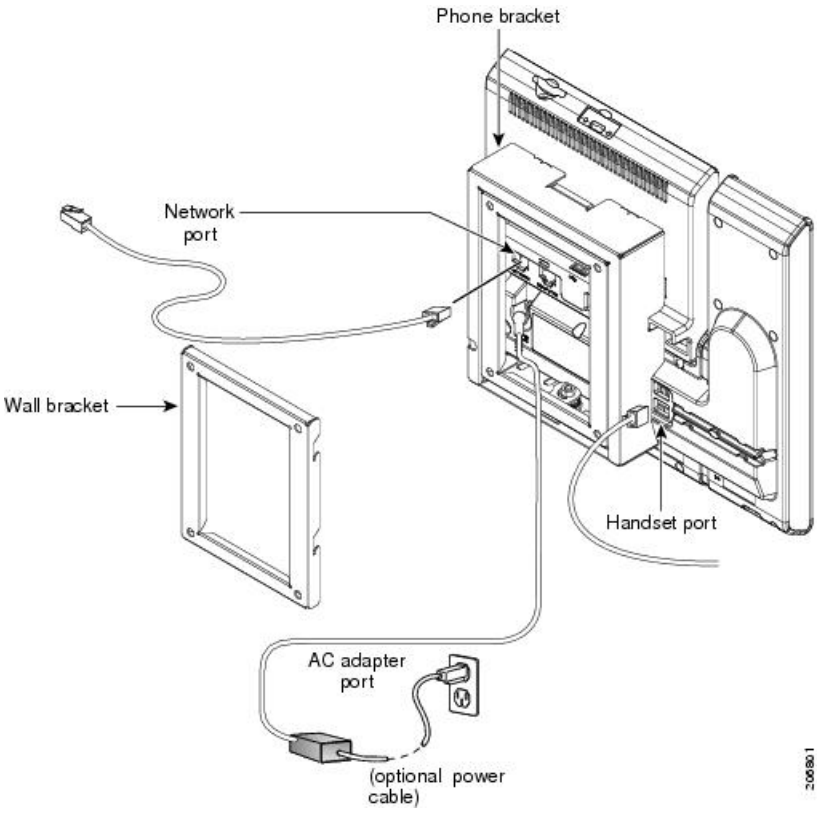


Step 3 Attach the cables to the phone:

a) Attach the Ethernet cable to the 10/100/1000 SW network port and wall jack.
b) (Optional) If you are connecting a network device (such as a computer) to the phone, attach the cable to the 10/100/1000 Computer (PC access) port.
c) (Optional) If you are using an external power supply, plug the power cord into the phone and dress the cord by clipping it into the clips that are incorporated into the phone body next to the PC port.
d) (Optional) If the cables terminate inside the wall bracket, connect the cables to the jacks.

The following figure shows the cables.

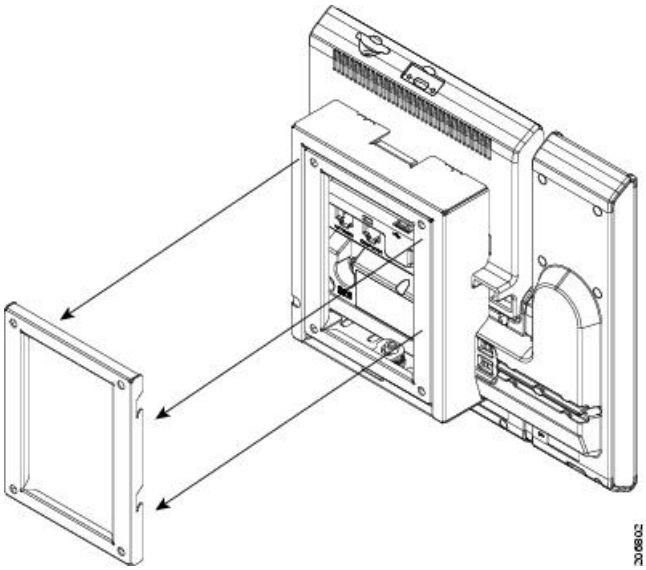
Figure 21: Attach Cables



Step 4 Attach the phone to the wall bracket by inserting the tabs on the top of the phone bracket into the slots on the wall bracket.
For cables that terminate outside of the brackets, use the cable-access openings in the bottom of the bracket to position the power cord and any other cable that does not terminate in the wall behind the bracket. The phone and wall bracket openings together form circular openings with room for one cable per opening.

The following figure shows how you attach the phone to the wall bracket.

Figure 22: Attach Phone to Wall Bracket



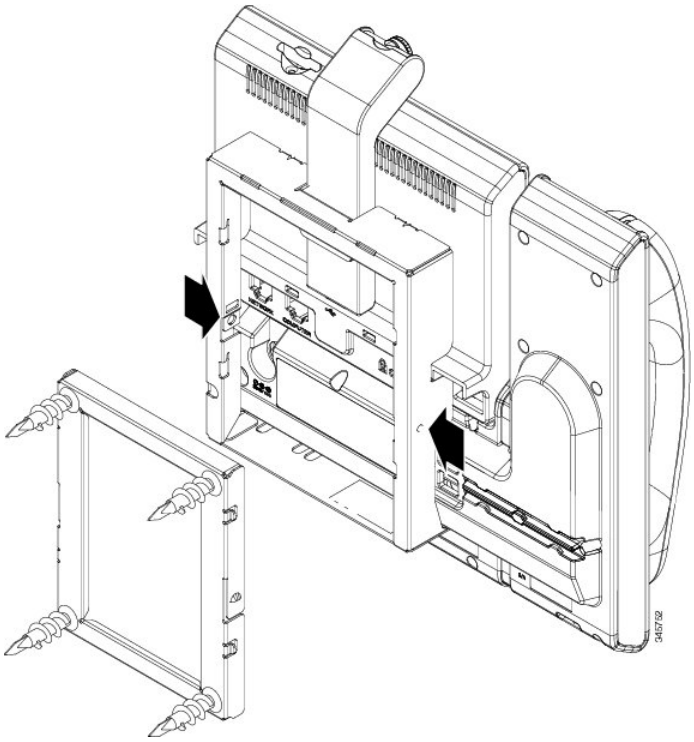
Step 5 Press the phone firmly into the wall bracket and slide the phone down. The tabs in the bracket click into position.

Step 6 Proceed to Adjust Handset Rest, on page 324.

Remove Phone from Non-Lockable Wall Mount

The phone mounting plate contains two tabs to lock the plate into the wall bracket. The following figure shows the location and shape of the tabs.

Figure 23: Tab Location



To remove the phone and mounting plate from the wall bracket, you must disengage these tabs.

Before You Begin

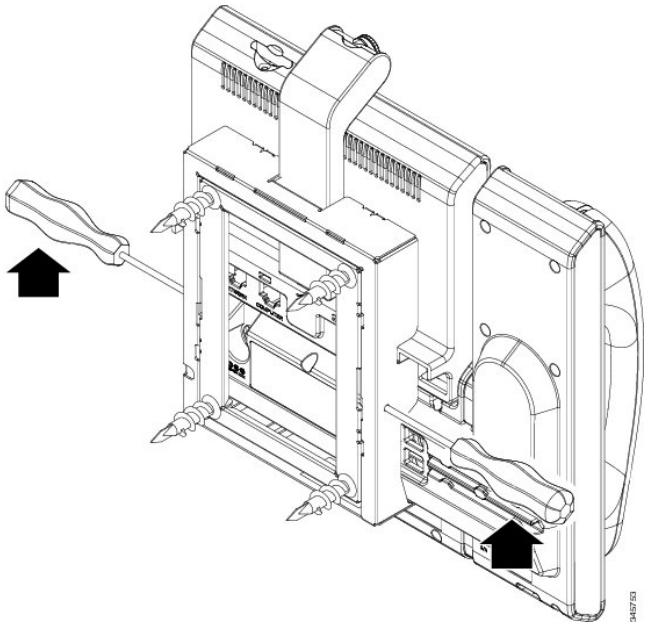
You require 2 screwdrivers or metal rods.

Procedure

Step 1 Push the screw drivers into the left and right holes in the phone mounting plate approximately 1 in. (2.5 cm).

Step 2 Lift the screwdriver handles up to put a downward pressure on the tabs.

Figure 24: Disengage Tabs



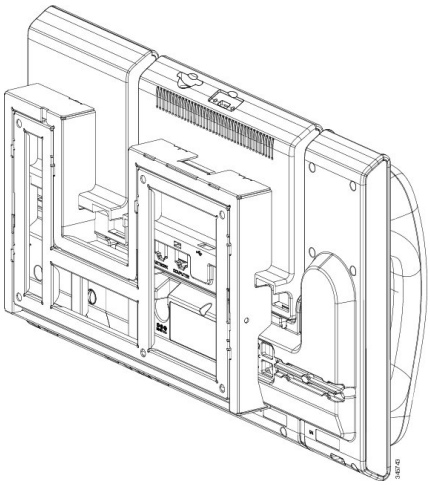
Step 3 Press firmly to disengage the tabs and lift the phone at the same time to release the phone from the wall bracket.

ADA Non-Lockable Wall Mount Kit for 8961 Series and 9900 Series IP Phones with Key Expansion Module

This section describes how to install the non-lockable wall mount kit on a Cisco Unified IP Phone 8961, 9951, and 9971 when the phone is connected to a Key Expansion Module.

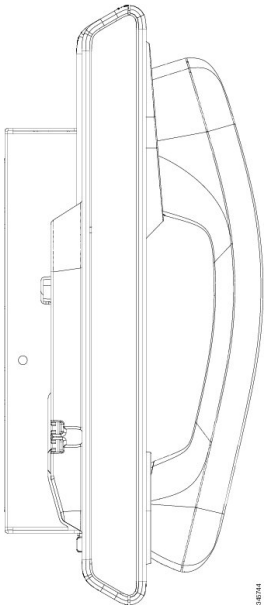
The following figure shows the wall mount kit installed on the phone.

Figure 25: Back View of ADA Non-Lockable Wall Mount Kit Installed on Phone with Key Expansion Module



The following figure shows the phone with the wall mount kit from the side.

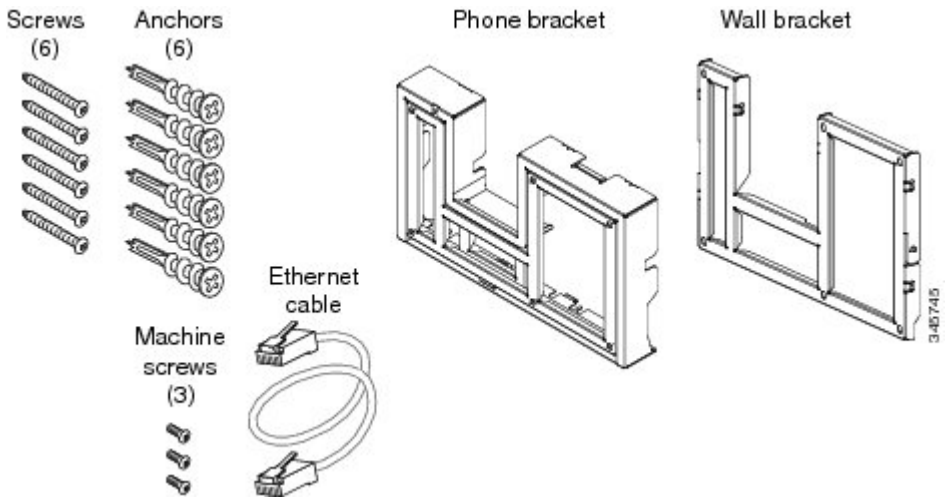
Figure 26: Side View of ADA Non-Lockable Wall Mount Kit Installed on Phone with Key Expansion Module



Components

The following figure shows the components of the ADA Non-Lockable Wall Mount Kit for the Cisco Unified IP Phone 8961, 9951, and 9971 with a Key Expansion Module.

Figure 27: Components



The package contains the following items:

- One phone bracket
- One wall bracket
- Six #8-18 x 1.25-inch Phillips-head screws with six anchors
- Three #4-40 x 0.31-inch machine screws
- One 6-inch Ethernet cable

Before You Begin

You need these tools to install the bracket:

- #1 and #2 Phillips-head screwdrivers
- Level
- Pencil

You must also install an Ethernet jack for the telephone in the desired location if an Ethernet jack does not currently exist. This jack must be wired appropriately for an Ethernet connection. You cannot use a regular telephone jack. For more information about phone installation requirements and warnings, see Cisco Unified IP Phone Installation, on page 38 and Cisco Unified IP Color Key Expansion Module Setup, on page 71.

Install Non-Lockable Wall Mount Kit for Phone with Key Expansion Module

The wall mount kit can be mounted on most surfaces, including concrete, brick, and similar hard surfaces. To mount the kit on concrete, brick, or similar hard surfaces, you must provide the appropriate screws and anchors for your wall surface.

Procedure

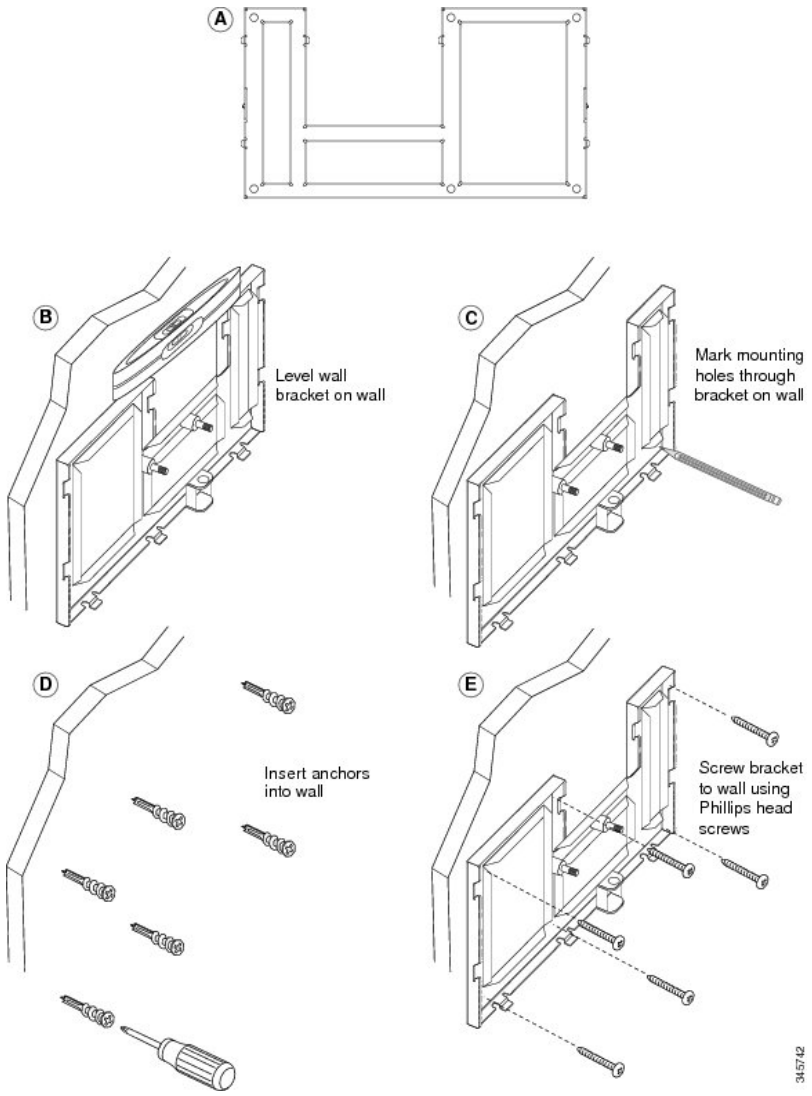
Step 1 Mount the wall bracket in the desired location. You can install the bracket over an Ethernet jack, or you can run the Ethernet network cable to a nearby jack.

Note If the jack is to be placed behind the phone, the Ethernet jack must be flush to the wall or recessed.

a) Hold the bracket on the wall. See the following figure for the orientation of the wall bracket.
b) Use the level to ensure that the bracket is level and use a pencil to mark the screw holes.
c) Using a #2 Phillips-head screwdriver, carefully center the anchor over the pencil mark and press the anchor into the wall.
d) Screw the anchor clockwise into the wall until it is seated flush.
e) Use the included screws and a #2 Phillips-head screwdriver to attach the bracket to the wall.

The following figure shows the steps for installing the bracket.

Figure 28: Bracket Installation



Step 2 Attach the phone bracket to the IP phone and key expansion assembly.

a) Detach the handset cord (and headset cord, if there is a headset), power cord, and any other attached cords from the base of the phone

b) Remove the label covers that are conceal the screw holes.

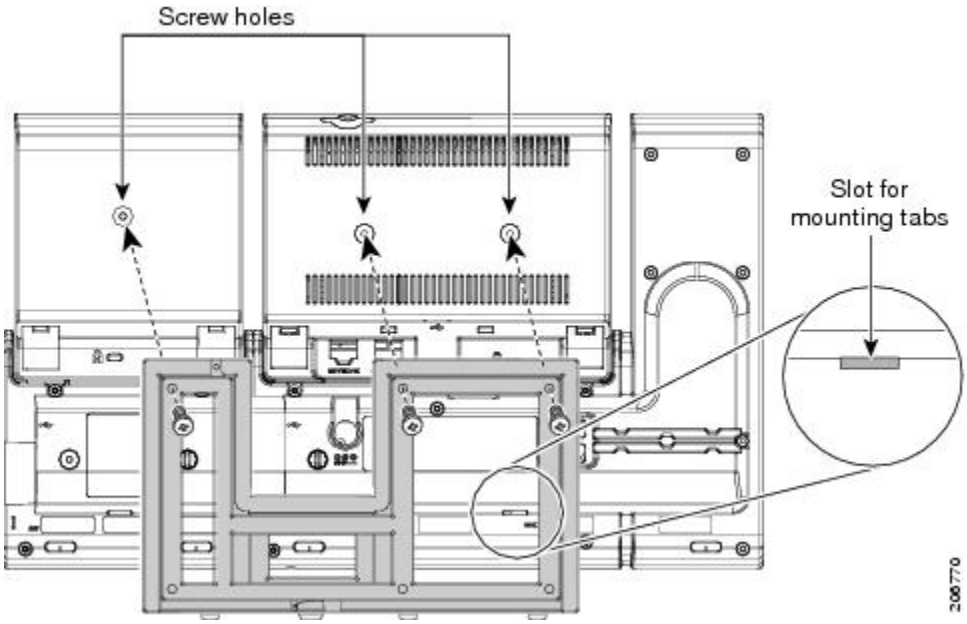
c) Attach the phone bracket by inserting the tabs into the mounting tabs on the back of the phone. The phone ports should be accessible through the holes in the bracket.

d) Secure the phone bracket to the IP phone with the machine screws using a #1 Philips-head screwdriver.

e) Thread the handset cord (and headset cord, if using one). Reattach the cords and seat them in the clips that are incorporated into the phone body.
The headset and handset connectors should be accessible from outside the wall mount bracket.

The following figure shows the steps to attach the phone bracket.

Figure 29: Attach Phone Bracket



Step 3 Attach the cords.

a) Attach the Ethernet cable to the 10/100/1000 SW network port and wall jack.

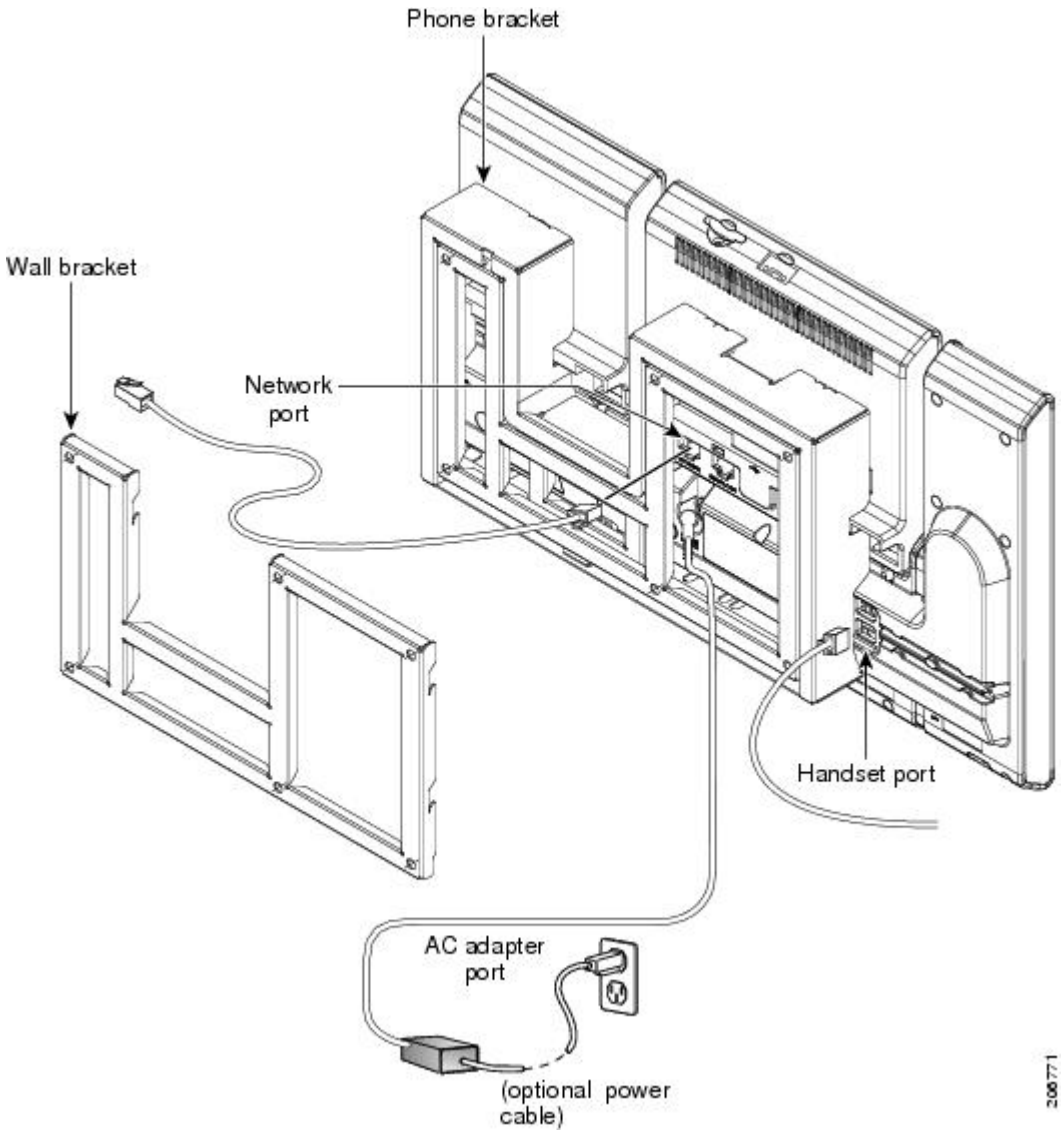
b) (Optional) If you are connecting a network device (such as a computer) to the phone, attach the cable to the 10/100/1000 Computer (PC access) port.

c) (Optional) If you are using an external power supply, plug the power cord into the phone and dress the cord by clipping it into the clips that are incorporated into the phone body next to the PC port.

d) (Optional) If the cables terminate inside the wall bracket, connect the cables to the jacks.

The following figure shows the cables.

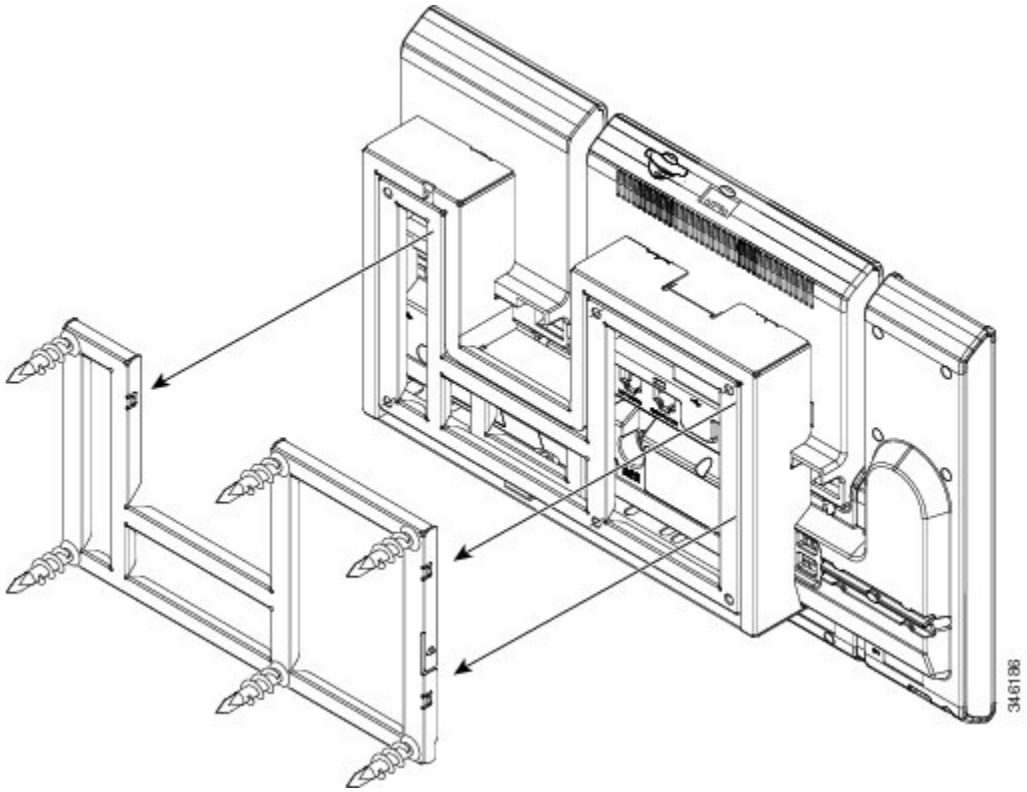
Figure 30: Attach Cables



Step 4 Attach the phone to the wall bracket by inserting the tabs on the top of the phone bracket into the slots on the wall bracket.

For cables that terminate outside of the bracket, use the cable-access openings in the bottom of the bracket to position the power cord and any other cable that does not terminate in the wall behind the bracket. The phone and wall bracket openings together form circular openings with room for one cable per opening.

Figure 31: Attach Phone to Wall Bracket

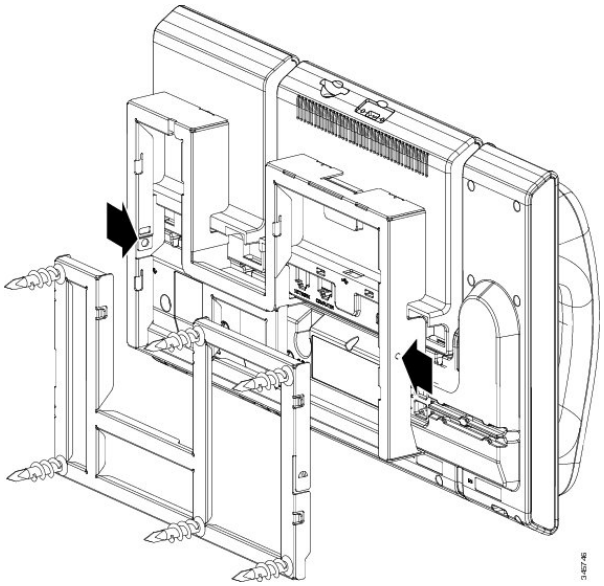


Step 5 Proceed to Adjust Handset Rest, on page 324.

Remove Phone and Key Expansion Module from Non-Lockable Wall Mount

The phone mounting plate contains two tabs to lock the plate into the wall bracket. The following figure shows the location and shape of the tabs.

Figure 32: Tab Location



To remove the phone and mounting plate from the wall bracket, you must disengage these tabs.

Before You Begin

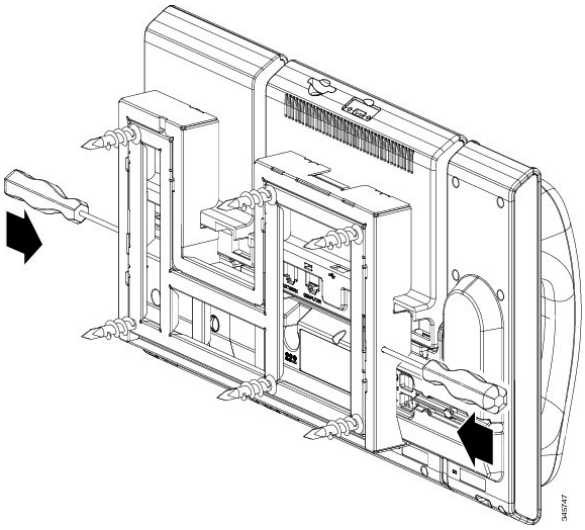
You require two screwdrivers or metal rods.

Procedure

Step 1 Push the screw drivers into the left and right holes in the phone mounting plate until you feel resistance.

Step 2 Press firmly inwards (towards the phone) to disengage the tabs, lift up on the phone to release the phone from the wall bracket, and then pull the phone towards you.

Figure 33: Disengage Tabs



INDEX

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X