# Cisco Unified IP Conference Phone 8831 and 8831NR Administration Guide

**First Published:** 2014-11-20

**Last Modified:** 2020-07-10

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

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

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

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

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

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

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

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

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

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

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

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

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

# CONTENTS

CHAPTER 1

# Preface

## Overview

The *Cisco Unified IP Conference Phone 8831 and 8831NR Administration Guide for Cisco Unified Communications Manager* provides the information you need to understand, install, configure, manage, and troubleshoot the Cisco Unified IP Conference Phone 8831 and 8831NR on a VoIP network.

Because of the complexity of a Unified Communications 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, or telecom engineers should review this guide to learn the steps required to properly set up the phone on the network.

The tasks described are administration-level tasks and are not intended for end users of the phones. Many of the tasks involve configuring network settings and affect the ability of the phone to function in the network.

Because of the close interaction between the phone and Cisco Unified Communications Manager, many of the tasks in this manual require familiarity with Cisco Unified Communications Manager.

## Organization

This manual is organized as follows.

| Chapter | Description |
|---|---|
| Cisco Unified IP Conference Phone 8831 and 8831NR, on page 9 | Provides a conceptual overview and description of the phone. |
| Cisco Unified IP Phones and Telephony Networks, on page 33 | Describes how to install the phone, and provides an overview of the tasks required prior to installation. |
| Cisco Unified IP Conference Phone Installation, on page 43 | Describes how to properly and safely install and configure the phone on your network. |
| Cisco Unified IP Conference Phone Settings, on page 59 | Describes how to configure network, device, and security settings on the phone. |
| Features, Templates, Services, and User Setup, on page 73 | Provides an overview of procedures for configuring telephony features, configuring directories, configuring conference phone button and softkey templates, setting up services, and adding users to Cisco Unified Communications Manager. |
| Cisco Unified IP Conference Phone Customization, on page 101 | Explains how to customize configuration files, ring sounds, and the idle display for the phone. |
| Model Information, Status, and Statistics, on page 105 | Explains how to view model, device, and network information from the phone. |
| Remote Monitoring, on page 111 | Describes the information that you can obtain from the phone web page. |
| Troubleshooting and Maintenance, on page 121 | Provides tips for troubleshooting the phone. |
| Internal Support Website, on page 139 | Provides suggestions for setting up a website for providing users with important information about their phone. |
| International User Support, on page 143 | Provides information about setting up phones in non-English environments. |
| Technical Specifications, on page 145 | Provides technical specifications for the phone. |

# Related Documentation

Use the following sections to obtain related information.

## Cisco Unified IP Conference Phone 8831 Documentation

The latest Cisco Unified IP Conference Phone 8831 documentation is available at the following URL:

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

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

## Cisco Business Edition 5000 Documentation

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

https://www.cisco.com/c/en/us/support/unified-communications/business-edition-5000/tsd-products-support-series-home.html

## Troubleshooting Documentation

Troubleshooting assistance is available to registered Cisco.com users at the following URL:

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

See the document *Using the 79xx Status Information For Troubleshooting*.

# Documentation, Support, and Security Guidelines

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

http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

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

# Cisco Product Security Overview

This product contains cryptographic features and is subject to 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. |
| `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.

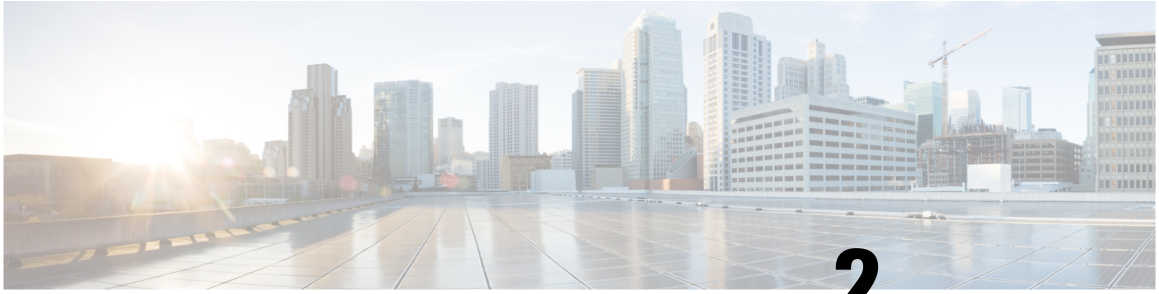
**Caution** Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

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 2

# New and Changed Information

## New and Changed Information for Firmware Release 10.3(1)SR6

| Feature | Impacted Section |
|---|---|
| TLS Enhancements | Actually introduced in 10.3(1)SR3.<br>Available Telephony Features, on page 74 |

## New Information for Firmware Release 10.3(1)SR3

| Feature | New Information |
|---|---|
| Cisco Unified IP Conference Phone 8831NR support | Cisco Unified IP Conference Phone 8831 and 8831NR Overview, on page 9<br>Supported Features, on page 18<br>Wireless Microphone Region Setting, on page 44<br>Wireless Extension Microphone Kit, on page 47<br>Wireless Microphone Menu, on page 51<br>Button Templates, on page 89<br>Linked Mode, on page 98<br>Physical and Operating Environment Specifications, on page 145 |
| Missing content | EnergyWise Mode, on page 37<br>Intermittent Network Outages, on page 125 |

CHAPTER 3

# Cisco Unified IP Conference Phone 8831 and 8831NR

## Cisco Unified IP Conference Phone 8831 and 8831NR Overview

The Cisco Unified IP Conference Phones 8831 and 8831NR are full-featured single line conference phones that provides voice communication over an IP network. They function much like a digital business phone, allowing you to place and receive calls and to access features such as mute, hold, transfer, call forward, and more. In addition, because conference phones connect to your data network, they offer enhanced IP telephony features, including access to network information and services, and customizable features and services. The conference phones also support certain security features.

The conference phone provides a backlit LCD screen and a variety of other sophisticated functions. Optional microphone extension kits provide enhanced room coverage that can be further expanded by linking two units together.

The Cisco Unified IP Conference Phone 8831 supports wired and wireless microphones. The Cisco Unified IP Conference Phone 8831NR supports only wired microphones.

The conference phone, like other network devices, must be configured and managed. The conference phones encode G.711a, G.711u, G.729a, G.722, G.729ab, iLBC, and decode all variants of G.711 and G.729. The conference phones also support 16-bit/16-kHz wideband audio.

⚠

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

# Buttons and Hardware

The Conference Phone has two primary components:

- Display Control Unit (DCU)
- Sound Base

In addition, the following optional extension kits can be added to or used with the conference phone:

- Wired Microphone Extension Kit
- Wireless Microphone Extension Kit and Charger

For your conference phone to work, it must be connected to the corporate IP telephony network.

## Display Control Unit

The Display Control Unit (DCU) is tethered to the Sound Base via a micro USB connector.

You can use the graphic and table below to identify buttons and hardware on the DCU.

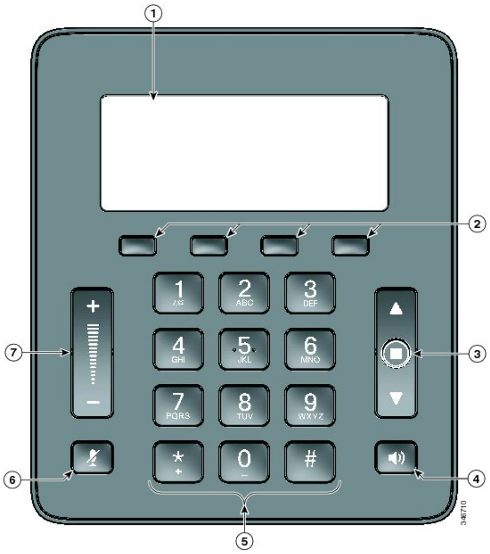


*Table 1: Display Control Unit Buttons and Softkeys*

| | Item | Description |
|---|---|---|
| 1 | Phone screen | LCD screen that displays conference phone menus and features. |
| 2 | Softkeys | Four programmable keys. |
| 3 | Navigation bar with Select key | 2-way Navigation bar and Select key that allows you to scroll menus and select items on the display. |

| | Item | Description |
|---|---|---|
| 4 | Call button | LED backlit call button.<br>Press this key to:<br>• Go Off Hook<br>• Answer an incoming call<br>• Obtain a dial tone to initiate a call<br>• Resume a call<br>• Release a call |
| 5 | Keypad | Allows you to dial phone numbers and enter letters. |
| 6 | Mute button | Toggles the Mute feature. A red backlight indicates a call is on mute. |
| 7 | Volume rocker | 2-way rocker switch that raises the volume of the speaker. |

**Note** For details on DCU LED behavior, see LED State Definitions, on page 12.

## Sound Base

The Sound Base provides 360 degree audio coverage via four built-in microphones and supports a full duplex speaker phone.

To provide enhanced room coverage, two sound base units can be linked together.

You can use the graphic and table below to identify buttons and connections on the Sound Base.

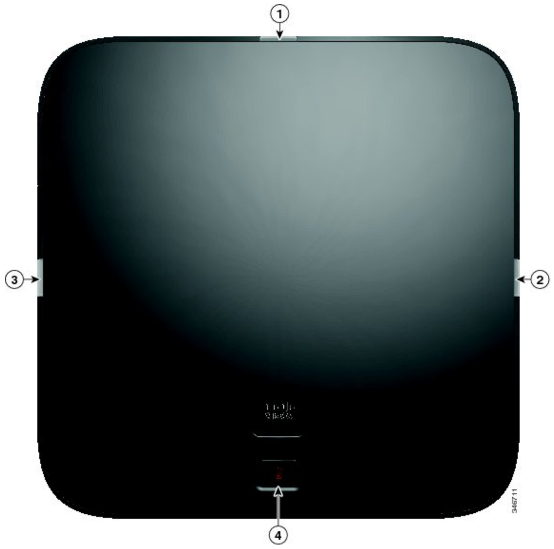


*Table 2: Sound Base Buttons*

| | Item | Description |
|---|---|---|
| 1, 2, 3 | LED indicators | Three LED indicators provide call status information. For details on LED behaviour, see LED State Definitions, on page 12. |
| 4 | Mute button<br>🔇 | Backlit mute button. |

# LED State Definitions

LEDs on the Sound Base and DCU provide information about the state of the conference phone.

For example, green flashing lights on the Sound Base and on the DCU Call button indicate that there is an incoming call. If the conference phone is on mute, then an incoming call will still flash green on the Call button, but the LED for the DCU mute button is solid red, the sound base LEDs are solid red, and the mute button on the Sound Base is also solid red.

The following table is a guide to the behaviour of the LEDs on the sound base and the DCU.

*Table 3: Conference Phone LED State Table*

| Media Path Status | Call on Focus | Sound Base | | | | Display Control Unit (DCU) | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Base LEDs (3) | | Mute Button | | DCU Call Button | | DCU Mute Button | |
| Off | No call | | | | | | | | |
| Off | No call, with VM | | | | | red | solid | | |
| Off | DND flash | green | flash | | | green | flash | | |
| Off | Incoming call | green | flash | | | green | flash | | |
| Off | Hold Revert Call | green | flash | | | green | flash | | |
| Off | Hold Call | green | pulse | | | green | pulse | | |
| Off | Hold Remote Call | | | | | red | pulse | | |
| Off | Remote in use Call | | | | | red | solid | | |
| Unmuted | Ringout/Connected Call | green | solid | | | green | solid | | |
| Unmuted | DNDFlash | green | solid | | | green | flash | | |
| Unmuted | Incoming Call | green | solid | | | green | flash | | |
| Unmuted | Hold Revert Call | green | solid | | | green | flash | | |
| Muted | Ringout/Connected | red | solid | red | solid | green | solid | red | solid |

| Media Path Status | Call on Focus | Sound Base | | | | Display Control Unit (DCU) | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Base LEDs (3) | | Mute Button | | DCU Call Button | | DCU Mute Button | |
| Muted | DND Flash | red | solid | red | solid | green | flash | red | solid |
| Muted | Incoming Call | red | solid | red | solid | green | flash | red | solid |
| Muted | Hold Revert Call | red | solid | red | solid | green | flash | red | solid |
| Deep Sleep Mode | Deep Sleep Mode | | | gray | solid | | | | |

# Phone Screen

The DCU contains the LCD phone screen. The idle or home screen displays information about the status of calls and features.

If the conference phone is in an offline state, the idle screen displays the message `Phone is not registered` and the **Apps** softkey remains available.

You can use the graphic and table below to identify the features and functions available on the screen.

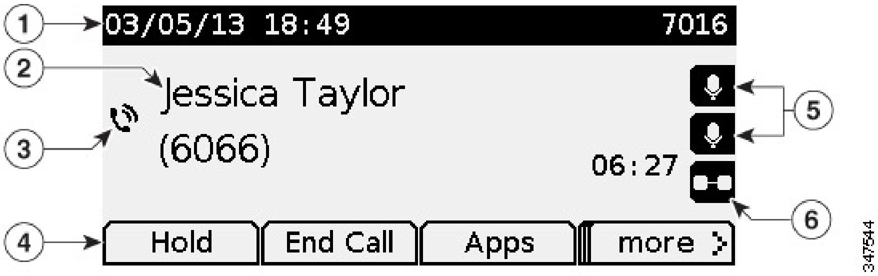


*Table 4: Phone Screen Layout.*

| | Item | Description |
|---|---|---|
| 1 | Header | Displays date, time, and current directory number. Displays menu name when applicable. |
| 2 | Line details and other phone information | Displays line label, call details, and status messages such as missed calls, message waiting, and line forwarding information. |
| 3 | Call State icon | Indicates the status of a call, such as ringing, hold, encrypted or connected call. |
| 4 | Softkey labels | Displays softkeys for currently available features or actions. |

| | Item | Description |
|---|---|---|
| 5, 6 | Feature icons | These icons are displayed when an associated feature, such as extension microphones (5) or Link mode (6) is connected. |

### Phone Screen Icons

*Table 5: Phone Screen Icons*

| Icon | Description |
|---|---|
| ☎ | On hook |
| 📞 | Off hook |
| ☎☎ | Ringing in |
| 📞 | Connected |
| ⏸ | Hold |
| 📞 | Shared line |
| 🎤 | Microphone connected |
| ▣ | Linked mode |
| 🔒 | Encrypted |

# Network Protocols

Cisco Unified IP Conference Phones support several industry-standard and Cisco networking protocols required for voice communication. The following table provides an overview of the networking protocols that the Cisco Unified IP Conference Phone supports.

*Table 6: Supported Networking Protocols on the Cisco Unified IP Conference Phone*

| Networking Protocol | Purpose | Usage Notes |
|---|---|---|
| Cisco Discovery Protocol (CDP) | CDP is a device-discovery protocol that runs on all Cisco-manufactured equipment.<br>Using CDP, a device can advertise its existence to other devices and receive information about other devices in the network. | The Cisco Unified IP Conference 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. |
| Dynamic Host Configuration Protocol (DHCP) | DHCP dynamically allocates and assigns an IP address to network devices.<br>DHCP enables you to connect an IP phone into the network and have the phone become operational without your needing 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.<br>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, go to the “Dynamic Host Configuration Protocol” chapter and the “Cisco TFTP” chapter in the *Cisco Unified Communications Manager System Guide*.<br>**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:<br>• Configuration file downloads<br>• XML services<br>• Firmware upgrades<br>• Troubleshooting purposes |

| Networking Protocol | Purpose | Usage Notes |
|---|---|---|
| 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.<br>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. | Cisco Unified IP Conference Phone implements the IEEE 802.1X standard by providing support for EAP-FAST and EAP-TLS authentication. |
| Internet Protocol (IP) | IP is a message protocol that addresses and sends packets across the network. | To communicate using IP, network devices must have an assigned IP address, subnet, and gateway.<br>IP addresses, subnets, and gateways identifications are automatically assigned if you are using the Cisco Unified IP Conference Phone with Dynamic Host Configuration Protocol (DHCP). If you are not using DHCP, you must manually assign these properties to each phone locally.<br>For more information, see the *Cisco Unified Communications Manager Features and Services Guide*. |
| Link Layer Discovery Protocol-Media Endpoint Devices (LLDP-MED) | LLDP-MED is an extension of the LLDP standard developed for voice products. | The Cisco Unified IP Conference Phone supports LLDP-MED on the SW port to communicate information such as:<br>• Voice VLAN configuration<br>• Device discovery<br>• Power management<br>• Inventory management<br>For more information about LLDP-MED support, see the *LLDP-MED and Cisco Discovery Protocol* white paper: http://www.cisco.com/en/US/technologies/tk652/tk701/technologies_white_paper0900aecd804cd46d.html |

| Networking Protocol | Purpose | Usage Notes |
|---|---|---|
| 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. |
| Real-Time Control Protocol (RTCP) | RTCP works in conjunction with RTP to provide QoS data (such as jitter, latency, and round trip delay) on RTP streams. | RTCP is disabled by default, but you can enable it on a per phone basis by using Cisco Unified Communications Manager. |
| Session Initiation Protocol (SIP) | SIP is the Internet Engineering Task Force (IETF) standard for multimedia conferencing over IP. SIP is an ASCII-based application-layer control protocol (defined in RFC 3261) that can be used to establish, maintain, and terminate calls between two or more endpoints. | Like other VoIP protocols, SIP is designed to address the functions of signaling and session management within a packet telephony network. Signaling allows call information to be carried across network boundaries. Session management provides the ability to control the attributes of an end-to-end call. |
| Secure Real-Time Transfer Protocol (SRTP) | SRTP is an extension of the Real-Time Protocol (RTP) Audio/Video Profile and ensures the integrity of RTP and Real-Time Control Protocol (RTCP) packets providing authentication, integrity, and encryption of media packets between two endpoints. | Cisco Unified IP Phones use SRTP for media encryption. |
| 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. | When security is implemented, Cisco Unified IP Conference Phone use the TLS protocol when securely registering with Cisco Unified Communications Manager.<br>For more information, see *Cisco Unified Communications Manager Security Guide*. |

| Networking Protocol | Purpose | Usage Notes |
|---|---|---|
| Trivial File Transfer Protocol (TFTP) | TFTP allows you to transfer files over the network.<br>On the Cisco Unified IP Conference Phone , TFTP enables you to obtain a configuration file specific to the phone type. | TFTP requires a TFTP server in your network, which can be automatically identified from the DHCP server. If you want a phone to use a TFTP server other than the one specified by the DHCP server, you must manually assign the IP address of the TFTP server by using the Network Setup menu on the phone.<br>For more information, see “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. | Cisco Unified IP Phones transmit and receive RTP streams, which utilize UDP. |

**Related Topics**

Cisco Unified IP Communications Product Interactions, on page 33

Phone Startup Process, on page 38

Network Setup Menu, on page 62

# Supported Features

The Cisco Unified IP Conference Phones 8831 and 8831NR function much like digital business or conference phones, and allow you to place and receive teleconference phone calls. In addition to traditional telephony features, the conference phone includes features that enable you to administer and monitor the conference phone as a network device.

The Cisco Unified IP Conference Phone 8831 supports wired and wireless microphones. The Cisco Unified IP Conference Phone 8831NR supports only wired microphones.

## Feature Overview

The Cisco Unified IP Conference Phone not only provides traditional telephony functionality, such as call forward and transfer, redial, and voice message system access, but it supports a full range of conference features. The conference phone also offers support for a variety of other features, such as WebDialer.

As with other network devices, the conference phone must be configured in order to access Cisco Unified Communications Manager and the rest of the IP network. By using DHCP for this process, you have fewer settings to configure on a device, but if your network requires it, an IP address, the TFTP server, and subnet information can be configured manually.

Conference 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 devices. 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 conference 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 conference phone.

### Related Topics

Cisco Unified IP Conference Phone Settings, on page 59
Features, Templates, Services, and User Setup, on page 73
Troubleshooting and Maintenance, on page 121

## Telephony Feature Administration

You can modify additional settings for the Cisco Unified IP Conference Phone from Cisco Unified Communications Manager Administration. Use Cisco Unified Communications Manager Administration to set up phone registration criteria and calling search spaces, to configure corporate directories and services, and to modify phone button templates, among other tasks.

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

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

http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-documentation-roadmaps-list.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

Available Telephony Features, on page 74

## Network Parameters

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

- IP address
- IP subnet information
- TFTP server IP address
- You also may configure the domain name and the DNS server settings, if necessary.

Collect this information and see the instructions in Cisco Unified IP Conference Phone Settings, on page 59.

### Related Topics

Model Information, Status, and Statistics, on page 105

## Information for End Users

If you are a system administrator, you are likely the primary source of information for conference phone users within your network or company. To ensure that you distribute the most current feature and procedural information, familiarize yourself with conference phone documentation. Make sure to visit the Cisco Unified IP Phone 8800 web site:

http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-user-guide-list.html

From this site, you can access various user guides and documentation.

In addition to providing users with documentation, it is important to inform them about available conference phone features, including features specific to your company or network, as well as how to access and customize those features, if appropriate.

### Related Topics

Internal Support Website, on page 139

# Cisco Unified IP Conference Phone Security Features

Implementing security in the Cisco Unified Communications Manager system prevents identity theft of the conference phone and Cisco Unified Communications Manager server and prevents data tampering.

To alleviate these threats, the Cisco IP telephony network establishes and maintains secure 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 Conference Phone uses the Phone Security profile, which defines whether the device is nonsecure or encrypted. For information on applying the security profile to the conference phone, see *Cisco Unified Communications Manager Security Guide*.

If you configure security-related settings in Cisco Unified Communications Manager Administration, the phone configuration file will contain sensitive information. To ensure the privacy of a configuration file, you must configure it for encryption. For detailed information, see “Configuring Encrypted Phone Configuration Files” chapter in *Cisco Unified Communications Manager Security Guide*.

The following table shows where you can find additional information about security.

***Table 7: 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 *Cisco Unified Communications Manager Security Guide*. |
| Security features supported on the Cisco Unified IP Conference Phone | See Supported Security Features, on page 22. |
| Restrictions regarding security features | See Security Restrictions, on page 27. |
| Viewing a security profile name | See Security Profiles, on page 24. |
| Identifying calls for which security is implemented | Encrypted Phone Call Identification. |

| Topic | Reference |
|---|---|
| TLS connection | See:<br>• Network Protocols, on page 14<br>• Cisco Unified Communications Manager IP Phone Addition Methods, on page 39 |
| Security and the conference phone startup process | See Phone Startup Process, on page 38. |
| Security and phone configuration files | See Cisco Unified Communications Manager IP Phone Addition Methods, on page 39. |
| Changing the TFTP Server 1 or TFTP Server 2 option on the conference phone when security is implemented | See IPv4 Setup Menu Options, on page 64. |
| Items on the Security Configuration menu that you access from the Device Configuration menu on the conference phone | See Security Setup Menu, on page 69. |
| Items on the Security Configuration menu that you access from the Settings menu on the conference phone | See Security Setup Menu, on page 69. |
| Applying a password to the phone so that no changes can be made to the administrative options | See Password Protection, on page 61. |
| Disabling access to conference phone web pages | See Control Web Page Access, on page 113. |
| Troubleshooting | See *Cisco Unified Communications Manager Security Guide*, “Troubleshooting” chapter. |
| Deleting the CTL file from the conference phone | See Cisco Unified IP Conference Phone Reset or Restore, on page 134. |
| Reset or restore the conference phone | See Cisco Unified IP Conference Phone Reset or Restore, on page 134. |
| 802.1X Authentication | See:<br>• 802.1X Authentication, on page 27<br>• Security Setup Menu, on page 69<br>• Status Menu, on page 106 |

**Note** All Cisco Unified IP Phones that support Cisco Unified Communications Manager use a security profile, which defines whether the phone is nonsecure or secure.

For information about configuring the security profile and applying the profile to the phone, see *Cisco Unified Communications Manager Security Guide*.

# Supported Security Features

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

For information about current security settings on a conference phone, choose **Apps** > **Admin Settings** > **Security Setup**.

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

*Table 8: Overview of Security Features*

| Feature | Description |
|---|---|
| Image authentication | Signed binary files (with the extension `.sebn`) prevent tampering with the firmware image before it is loaded on a conference phone. Tampering with the image causes a phone to fail the authentication process and reject the new image. |
| Customer-site certificate installation | Each conference phone requires a unique certificate for device authentication. Conference phones include a manufacturing installed certificate (MIC), but for additional security, you can specify in Cisco Unified Communications Manager Administration that a certificate be installed by using the Certificate Authority Proxy Function (CAPF). Alternatively, you can install a Locally Significant Certificate (LSC) from the Security Configuration menu on the phone. |
| Device authentication | Occurs between the Cisco Unified Communications Manager server and the conference phone when each entity accepts the certificate of the other entity. Determines whether a secure connection between the conference 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 will not register conference phone unless they can be authenticated by the Cisco Unified Communications Manager. |

| Feature | Description |
|---|---|
| File authentication | Validates digitally signed files that the conference phone downloads. The conference phone validates the signature to make sure that file tampering did not occur after the file creation. Files that fail authentication are not written to Flash memory on the conference phone. The conference phone rejects such files without further processing. |
| Signalling Authentication | Uses the TLS protocol to validate that no tampering has occurred to signalling packets during transmission. |
| Manufacturing installed certificate | Each conference phone contains a unique manufacturing installed certificate (MIC), which is used for device authentication. The MIC is a permanent unique proof of identity for the conference phone, and allows Cisco Unified Communications Manager to authenticate the phone. |
| Secure SRST reference | After you configure a SRST reference for security and then reset the dependent devices in Cisco Unified Communications Manager Administration, the TFTP server adds the SRST certificate to the `cnf.xml` file and sends the file to the phone. A secure phone then uses a TLS connection to interact with the SRST-enabled router. |
| Media encryption | Uses SRTP to ensure that the media streams between supported devices proves secure and that only the intended device receives and reads the data. Includes creating a media primary 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 conference phone, and interacts with the conference phone for key generation and certificate installation. The CAPF can be configured to request certificates from customer-specified certificate authorities on behalf of the conference phone, or it can be configured to generate certificates locally. |
| Security profiles | Defines whether the conference phone is nonsecure or encrypted. |
| Encrypted configuration files | Allows you to ensure the privacy of phone configuration files. |
| Optional disabling of the web server functionality for a conference phone | You can prevent access to a conference phone web page, which displays a variety of operational statistics for the conference phone. |

| Feature | Description |
|---|---|
| Phone hardening | Additional security options, which you control from Cisco Unified Communications Manager Administration:<br>• Disabling access to web pages for a phone |
| 802.1X Authentication | The Cisco Unified IP Conference Phone 8831 can use 802.1X authentication to request and gain access to the network. |

### Related Topics

Security Profiles, on page 24

802.1X Authentication and Status Menus, on page 71

Cisco Unified IP Conference Phone Settings, on page 59

# Security Profiles

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

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

### Related Topics

Security Setup Menu, on page 69

# Encrypted Phone Call Identification

When security is enabled for a phone, a lock icon is displayed on the phone screen during an encrypted call. 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 encrypted audio. If your call is connected to a non-protected phone, the security tone does not play.

In a secure call, all call signalling and media streams are encrypted. An encrypted call offers a high level of security, providing integrity and privacy to the call. When a call in progress is being encrypted, the call icon on the phone screen changes to the lock icon: 🔒.

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.

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

## Initiate Secure Conference Call

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

**Procedure**

**Step 1** A user initiates the conference from a secure conference phone.

**Step 2** Cisco Unified Communications Manager assigns a secure conference bridge to the call.

**Step 3** As participants are added, Cisco Unified Communications Manager verifies the security mode of each phone and maintains the security level for the conference.

There are interactions, restrictions, and limitations that affect the security level of the conference call depending on the security mode of the participant phones and the availability of secure conference bridges. For more information about the interactions, see Call Security Interactions and Restrictions, on page 25

**Step 4** If the conference call is secure the 🔒 icon is displayed on the screen.

## Initiate Secure Phone Call

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

A protected call is established using this process:

**Procedure**

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

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

**Step 3** A security tone plays if the call is connected to another protected phone, indicating that both ends of the conversation are encrypted and protected. If the call is connected to a unprotected phone, then the secure tone does not play.

**Note** Protected calling is supported for conversations between two phones. Some features, such as conference calling and Cisco Extension Mobility are not available when protected 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 9: Call Security Interactions When Using Barge*

| Initiator’s Phone Security Level | Feature Used | Call Security Level | Results of Action |
|---|---|---|---|
| Nonsecure | cBarge | Encrypted call | Call barged and identified as nonsecure call |
| Secure | cBarge | Secure call | Call barged and identified as Secure call |

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

*Table 10: Security Restrictions with Conference Calls*

| Initiator’s Phone Security Level | Feature Used | Security Level of Participants | Results of Action |
|---|---|---|---|
| Nonsecure | Conference | Encrypted | Nonsecure conference bridge<br>Nonsecure conference |
| Secure | Conference | At least one member is nonsecure. | Secure conference bridge<br>Nonsecure conference |
| Secure | Conference | All participants are encrypted. | Secure conference bridge<br>Secure encrypted level conference |
| Secure | Join | Encrypted | Secure conference bridge<br>Conference remains secure |
| Nonsecure | cBarge | All participants are encrypted. | Secure conference bridge<br>Conference changes to nonsecure |
| Nonsecure | Meet Me | Minimum security level is encrypted. | Only nonsecure conference bridge is available and used<br>Nonsecure conference |
| Secure | Meet Me | Minimum security level is nonsecure | Only secure conference bridge available and used<br>Conference accepts all calls |

# 802.1X Authentication

Cisco Unified IP Conference Phone supports 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.

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 EAP-FAST and EAP-TLS 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 another 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 best practices 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 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 multi-domain authentication, you can continue to use the voice VLAN.
    - Disabled: If the switch does not support multi-domain 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.

# Security Restrictions

A user cannot barge into an encrypted call if the phone that is used to barge is not configured for encryption. In this case, a reorder (fast busy) tone plays on the phone from which 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 Conference 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 complete Cisco IP telephony network, see the “System Configuration Overview” chapter in the *Cisco Unified Communications Manager System Guide*.

After the IP telephony system is setup and you have configured system-wide features in Cisco Unified Communications Manager, phones can be added to the system.

For an overview of procedures used to add phones to your network, see the “Installation” and “Setup in Cisco Unified Communications Manager” sections of this guide.

## Cisco IP Phone Setup in Cisco Unified Communications Manager

To add conference 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 more information about these choices, see Cisco Unified Communications Manager IP Phone Addition Methods, on page 39.

For general information about configuring conference phones in Cisco Unified Communications Manager, see

- “Cisco Unified IP Phones”, *Cisco Unified Communications Manager System Guide*
- “Cisco Unified IP Phone Configuration”, *Cisco Unified Communications Manager Administration Guide*
- “Autoregistration Configuration”,*Cisco Unified Communications ManagerAdministration Guide*

### Set Up the Cisco Unified IP Conference Phone in Cisco Unified Communications Manager Administration

The following steps provide an overview and checklist of configuration tasks for the conference station in Cisco Unified Communications Manager Administration. The steps present a suggested order to guide you through the conference phone configuration process. Some tasks are optional, depending on your system and user needs. For detailed information, see the sources listed.

### Procedure

**Step 1** Gather the following information about the conference station:

- Conference phone model
- MAC address
- Physical location of the conference station
- Name or user ID of conference station user
- Device pool
- Partition, calling search space, and location information
- Directory number assigned to the conference phone
- Cisco Unified Communications Manager user to associate with conference phone
- Conference phone usage information that affects conference station templates (button and softkey), features, services, or conference phone applications

Provides a list of configuration requirements for setting up conference phones and identifies preliminary configuration that you need to perform before configuring individual conference phones, such as conference phone key button templates or softkey templates. For more information, see the *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones" chapter and also refer to Available Telephony Features, on page 74.

**Step 2** Customize button templates (if required). Allows you to create a custom button template with the Privacy feature. You can assign this template to shared conference phones so users have access to the Privacy feature. For more information, see *Cisco Unified Communications Manager Administration Guide*, "Phone Button Template Configuration" chapter and Button Templates, on page 89.

**Step 3** Add and configure the conference phone. Adds the conference phone with its default settings to the Cisco Unified Communications Manager. For more information, see the *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Configuration" chapter. For more information about Product Specific Configuration fields, refer to the Help in the Phone Configuration window.

**Step 4** Add and configure directory number on the conference phone. Adds the directory number and features associated with the directory number to the conference phone. For more information, see the *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Configuration" chapter, "Directory Number Configuration" and "Creating a Cisco Unity Voice Mailbox" sections, and Available Telephony Features, on page 74.

**Step 5** Customize softkey templates to add, delete, or change the order of softkey features that display on the conference phone to meet feature needs. For more information, see the *Cisco Unified Communications Manager Administration Guide*, "Softkey Template Configuration" chapter, and Softkey Templates, on page 90.

**Step 6** (Optional) Configure conference phone services and assign services.

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

For more information, see the *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Services Configuration" chapter, and Services Setup, on page 95.

**Step 7** Add user information to the global directory for Cisco Unified Communications Manager. For more information, see the *Cisco Unified Communications Manager Administration Guide*, “Add a New User” chapter, and Cisco Unified Communications Manager User Addition, on page 95.

**Note** If your company uses a Lightweight Directory Access Protocol (LDAP) directory to store information on users, you can install and configure Cisco Unified Communications to use your existing LDAP directory, see Corporate Directory Setup, on page 89.

**Step 8** Associate a user to a user group with a conference phone. Provides users with control over their conference phone such as forwarding calls or adding services.

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

For more information, see the *Cisco Unified Communications Manager Administration Guide*, “Adding a New User” chapter, “Associate Devices with a User” section.

# Cisco Unified IP Conference Phone 8831 Installation

After you have added the phone to the Cisco Unified Communications Manager database, you can complete the installation. The conference phone can be installed at the user's location either by you, or by the user.

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

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

**Note** Upgrade the conference phone with the current firmware image before you install the phone. For information about upgrading, see the Readme file for the conference phone.

The conference phone supports seamless firmware upgrades. For instructions on upgrading the firmware, see the Release Notes.

These and other related documents can be located from http://www.cisco.com/en/US/products/ps12965/tsd_products_support_series_home.html.

## Install the Cisco Unified IP Conference Phone

The following steps provide an overview and checklist of installation tasks for the conference phone. The steps present a suggested order to guide you through the conference 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 conference phone:

- Power over Ethernet (PoE)
- External power supply

Determines how the conference phone receives power. For more information, see Conference Phone Power, on page 35.

**Step 2** Assemble the conference phone, adjust placement, and connect the network cable. Locates and installs the phone in the network. For more information, see Phone Connections, on page 48.

**Step 3** Monitor the conference phone startup process. Verifies that the conference phone is configured properly. For more information, see IP Phone Startup Verification, on page 53.

**Step 4** Configure these network settings on the conference phone by choosing **Apps** > **Settings** > **Network Configuration**.

**Step 5** To enable DHCP:

a) Set DHCP Enabled to **Yes**.
b) To use an alternate TFTP server, set Alternate TFTP to **Yes**.
c) Enter an IP address for TFTP Server 1.

With DHCP enabled, the IP address is automatically assigned and the conference phone is directed to a TFTP Server. Consult with the network administrator if you need to assign an alternative TFTP server instead of using the TFTP server assigned by DHCP.

For more information, see Network Settings, on page 54 and Network Setup Menu, on page 62.

**Step 6** To disable DHCP:

a) Set DHCP Enabled to **No**.
b) Enter a static IP address for the conference phone.
c) Enter the Subnet Mask.
d) Enter the IP address for Default Router 1.
e) Enter the Domain Name where the conference phone resides.
f) Set Alternate TFTP to **Yes**.
g) Enter an IP address for TFTP Server 1.

Without DHCP, you must configure the IP address, TFTP server, subnet mask, domain name, and default router locally on the conference phone.

For more information, see Network Settings, on page 54 and Network Setup Menu, on page 62.

**Step 7** Set up security on the conference phone. Provides protection against data tampering threats and identity theft of conference phones. For more information, see Security Setup Menu, on page 69.

**Step 8** Place calls with the conference phone. Verifies that the conference phone and features work correctly. For more information, see the phone user guide.

**Step 9** Provide information to end users about how to use their conference phones and how to configure their conference phone options. Ensures that users have adequate information to successfully use their conference phones. For more information, see Internal Support Website, on page 139.

# Terminology Differences

The following table highlights some of the important differences in terminology that is used in these documents:

- *Cisco Unified IP Conference Phone 8831 and 8831NR Administration Guide*
- *Cisco Unified IP Conference Phone 8831 and 8831NR User Guide*
- *Cisco Unified Communications Manager Administration Guide*
- *Cisco Unified Communications Manager System Guide*

***Table 11: Terminology Reference***

| User Guide | Administration and System Guides |
|---|---|
| Conference across Lines | Join Across Lines |
| Conference | Join or Conference |
| Line Status | Busy Lamp Field (BLF) |
| Message Indicators | Message Waiting Indicator (MWI) or Message Waiting Lamp |
| Programmable Feature Button | Programmable Line Button or Programmable Line Key (PLK) |
| Voicemail System | Voice Messaging System |

CHAPTER 4

# Cisco Unified IP Phones and Telephony Networks

## Phone and Telephony Networks Overview

The Cisco Unified IP Conference Phone enables you to communicate by using voice over a data network. To provide this capability, the conference phones depend upon and interact with several other key Cisco Unified IP Telephony components, including DNS and DHCP servers, TFTP servers, and switches.

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

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

This chapter provides an overview of the interaction between the conference phone and other key components of a Voice over IP (VoIP) network. It also describes options for powering conference phones.

## Cisco Unified IP Communications Product Interactions

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

### Interactions with Other Cisco Unified IP Telephony Products

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

## Cisco Unified IP Conference Phone and Cisco Unified Communications Manager Interaction

Cisco Unified Communications Manager is an open and industry-standard call processing system. Cisco Unified Communications Manager software sets up and tears down calls between IP devices, integrating traditional private branch exchange (PBX) functionality with the corporate IP network. Cisco Unified Communications Manager manages the components of the IP telephony system—the conference stations, 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 conference stations and phones
- Authentication and encryption (if configured for the telephony system)
- Configuration file using the TFTP service
- Conference phone registration
- Call preservation, so that a media session continues if signalling is lost between the primary Communications Manager and a conference phone

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

**Note** If the conference 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/cisco/software/navigator.html?mdfid=282677102&i=rm

For more information, see “Software Upgrades”, *Cisco Unified Communications Operating System Administration Guide*

**Related Topics**

Cisco Unified IP Conference Phone Security Features, on page 20
Available Telephony Features, on page 74

## Cisco Unified IP Conference Phone and VLAN Interaction

When Voice VLAN (VVLAN) is disabled, the egress SW port packets are not tagged and only untagged packets are accepted on the ingress direction.

When VVLAN is configured as 1-4094, the egress SW port packets are tagged with the VVLAN. For ingress packets, if VLAN is different from VVLAN, only the packets that match the VVLAN are accepted. If VLAN equals VVLAN then both packets that match the VVLAN and untagged packets are accepted.

When VVLAN is set to 0, 802.1p is enabled. The egress SW port packets will be tagged with 802.1p. On the ingress side, both 802.1p tagged packets and untagged packets are accepted.

For more information, see the documentation included with a Cisco switch. You can also access switch information at this URL: http://www.cisco.com/en/US/products/hw/switches/index.html

**Related Topics**

Phone Startup Process, on page 38

## Cisco Unified IP Conference Phone and Cisco Unified Communications Manager Express Interaction

If supported, when the phone works with the Cisco Unified Communications Manager Express (Unified CME), the phone must go into CME mode.

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

In CME mode, the conference phones either only partially support, or do not support the following actions:

*Table 12: Supported Phone Features for CME Mode*

| Action | Support Level |
|---|---|
| Barge | Not supported. |
| Conference | Only supported in the connected call transfer scenario. |
| Direct Transfer | Not supported. |
| Hold | Supported using the Hold softkey. |
| Join | Supported using the Conference softkey. |
| Select | Not supported. |
| Transfer | Only supported in the connected call transfer scenario. |

# Conference Phone Power

The Cisco Unified IP Conference Phone can be powered with external power or with Power over Ethernet (PoE). External power is provided through a separate power supply. PoE is provided by a switch through the Ethernet cable attached to a conference phone.

**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 powering the Cisco Unified IP Conference Phone.

*Table 13: Guidelines for Powering the Cisco Unified IP Conference Phone*

| Power Type | Guidelines |
|---|---|
| External power: Provided by an external power supply. | The Cisco Unified IP Conference Phone uses the CP-PWR-CUBE-3 external power supply.<br>When using a sound base in Linked Mode, the primary sound base must be connected using the CP-PWR-CUBE-3 external power supply. |

| Power Type | Guidelines |
|---|---|
| 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 or Conference Phone. It functions as a mid-span device to deliver inline power to the attached phone. The Cisco Unified IP Phone Power Injector is connected between a switch port and the IP Conference Phone and supports a maximum cable length of 100m between the unpowered switch and the IP Phone. |
| External power: Provided through inline power patch panel WS-PWR-PANEL. | The inline power patch panel WS-PWR-PANEL is compatible with the Cisco Unified IP Conference Phone. |
| PoE power: Provided by a switch through the Ethernet cable attached to the conference phone. | • The Cisco Unified IP Conference Phone supports IEEE 802.3af Class 3 power on signal pairs and spare pairs.<br>• When using a sound base in Linked Mode, the primary sound base must be connected using the CP-PWR-CUBE-3 external power supply.<br>• To ensure uninterruptible operation of the conference phone, make sure that the switch has a backup power supply.<br>• Make sure that the CatOS or IOS version running on your switch supports your intended conference phone deployment. Refer to the documentation for your switch for operating system version information. |

# 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 dialling 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 dialling.

# Power Reduction

You can reduce the amount of energy that the 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 interacts with the device. In the Device Configuration window on Cisco Unified Communications 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

The conference 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.

## Additional Power Information

For related information about power, see the documents listed in the following table. These documents provide information about these topics:

- Cisco switches that work with the conference phone
- The Cisco IOS releases that support bidirectional power negotiation
- Other requirements and restrictions regarding power

*Table 14: Related Power Documentation*

| Document Topics | URL |
|---|---|
| PoE Solutions | http://www.cisco.com/en/US/netsol/ns340/ns394/ns147/ns412/networking_solutions_package.html |
| Cisco Catalyst Switches | http://www.cisco.com/univercd/cc/td/doc/product/lan/index.htm |
| 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 conference 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 conference phone to be reset, a change is made to the conference phone configuration file automatically.

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

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

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

If autoregistration is not enabled and the phone has not been added to the Cisco Unified Communications Manager Database, the phone registration request will be rejected. In this case, the conference phone will reset and attempt to register repeatedly.

If the conference phone has registered before, the conference phone will access the configuration file named `SEPmac_address.cnf.xml`, where the `mac_address` portion of the filename is the Media Access Control (MAC) address of the conference phone.

# Phone Startup Process

When connecting to the VoIP network, the conference phone goes through a standard startup process, as described in the following table. Depending on your specific network configuration, not all of these process steps may occur on your conference phone.

1. Obtain power from the switch. If a conference phone is not using external power, the switch provides in-line power through the Ethernet cable attached to the conference phone. For more information, see Conference Phone Power, on page 35.

2. Load the stored conference phone image. The conference phone has non-volatile flash memory in which it stores firmware images and user-defined preferences. At startup, the conference phone runs a bootstrap loader that loads a conference phone image stored in flash memory. Using this image, the conference phone initializes its software and hardware. For more information, see .

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

4. Obtain an IP address . If the Cisco Unified IP Conference Phone uses DHCP to obtain an IP address, the phone queries the DHCP server to obtain one. If you do not use DHCP in your network, you must assign static IP addresses to each phone locally.

5. Access a TFTP server. In addition to assigning an IP address, the DHCP server directs the Cisco Unified IP Conference 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 alternative TFTP server to use instead of the one that DHCP assigns.

6. 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 conference phone. For more information, see Phone Configuration Files, on page 37.

7. Contact Cisco Unified Communications Manager. The configuration file defines how the conference phone communicates with Cisco Unified Communications Manager and provides a conference phone with its load ID. After obtaining the file from the TFTP server, the conference phone attempts to make a connection to the highest priority Cisco Unified Communications Manager on the list. The conference phone makes a non-secure TCP connection.

   If the conference phone was manually added to the database, Cisco Unified Communications Manager identifies the conference phone. If the conference phone was not manually added to the database and auto-registration is enabled in Cisco Unified Communications Manager, the conference phone attempts to auto-register itself in Cisco Unified Communications Manager.

   Auto-registration is disabled when security is enabled on Cisco Unified Communications Manager. In this case, the conference phone must be manually added to the Cisco Unified Communications Manager.

### Related Topics

Startup Problems, on page 121
Network Setup Menu, on page 62

# Cisco Unified Communications Manager IP Phone Addition Methods

Before installing the conference phone, you must choose a method for adding conference phones to Cisco Unified Communications Manager database. Be aware that each phone type requires a fixed number of device license units and the number of unit licenses that are available on the server may impact phone registration. For more information about licensing, see “Licenses for Phones” section in the *Cisco Unified Communications Manager System Guide*.

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

***Table 15: Methods for Adding IP Phones to Cisco Unified Communications Manager Database***

| Method | Requires MAC Address? | Notes |
|---|---|---|
| Autoregistration | No | Results in the automatic assignment of a directory number to the conference phone, and provides no control over directory number assignment to conference phones.<br>Not available when security or encryption is enabled. In this case, the conference phone must be manually added to the Cisco Unified Communications Manager database. |

| Method | Requires MAC Address? | Notes |
|---|---|---|
| Autoregistration with the Tool for Auto-Registered Phones Support (TAPS) | No | Requires autoregistration and the Bulk Administration Tool (BAT).<br>This method updates the Cisco Unified Communications Manager database with the MAC address and DNs for the device when user calls TAPS from the conference phone. |
| Using Cisco Unified Communications Manager Administration | Yes | Requires you to add conference phones individually. |
| Using BAT | Yes | Allows for the simultaneous registration of multiple conference phones of the same model.<br>Allows you to schedule when conference phones are added to Cisco Unified Communications Manager. |

# Autoregistration IP Phone Addition

If you enable autoregistration before you begin installing conference phones, you can:

- Automatically add a conference phone to the Cisco Unified Communications Manager database when you physically connect the conference phone to your IP telephony network. During autoregistration, Cisco Unified Communications Manager assigns the next available sequential directory number to the conference phone.
- Add conference phones without first gathering MAC addresses from the conference phones.
- Quickly enter conference phones into the Cisco Unified Communications Manager database and modify any settings, such as the directory numbers, from Cisco Unified Communications Manager.
- Move autoregistered conference 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 conference phones to your network. To add more than 100 conference 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 plan to implement authentication or encryption. For information about enabling autoregistration, see “Enable Autoregistration” section in the *Cisco Unified Communications Manager Administration Guide*. For information about authentication or encryption as it pertains to autoregistration, refer to *Cisco Unified Communications Manager Security Guide*.

**Note** When you configure the client 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, autoregistation is automatically enabled.

### Related Topics

- Autoregistration and TAPS IP Phone Addition, on page 41
- Cisco Unified Communications Manager Administration Conference Station Addition, on page 41
- BAT IP Phone Addition, on page 42

## Autoregistration and TAPS IP Phone Addition

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

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

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

To implement TAPS, dial a TAPS directory number and follow voice prompts. When the process is complete, the conference phone has downloaded the directory number (DN) and other settings. The conference phone has also been updated in Cisco Unified Communications Manager Administration with the correct MAC address.

Autoregistration must be enabled in Cisco Unified Communications Manager Administration for TAPS to function. You can do this from **System** > **Cisco Unified CM**.

**Note** When you configure the client 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, autoregistation is automatically enabled.

For more information, see “Bulk Administration”, *Cisco Unified Communications Manager Administration Guide* and “Tool for Auto-Registered Phones Support”, *Cisco Unified Communications Manager Bulk Administration Guide*.

### Related Topics

- Autoregistration IP Phone Addition, on page 40
- Cisco Unified Communications Manager Administration Conference Station Addition, on page 41
- BAT IP Phone Addition, on page 42

## Cisco Unified Communications Manager Administration Conference Station Addition

You can add conference 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 conference phone.

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

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

### Related Topics

Autoregistration IP Phone Addition, on page 40

Autoregistration and TAPS IP Phone Addition, on page 41

BAT IP Phone Addition, on page 42

Conference Phone MAC Address Determination, on page 42

# BAT IP Phone Addition

Cisco Unified Communications Manager Bulk Administration Tool (BAT) enables you to perform batch operations, including registration, on multiple conference phones. To access BAT, choose the Bulk Administration drop-down menu in Cisco Unified Communications Manager Administration.

Before you can add conference phones using BAT only (not in conjunction with TAPS), you must obtain the MAC address for each conference phone. If you have a large number of conference phones to register you can use dummy MAC addresses and update them later via TAPS.

For detailed instructions about using BAT, see “Bulk Administration”, *Cisco Unified Communications Manager Administration Guide*.

### Related Topics

Autoregistration IP Phone Addition, on page 40

Autoregistration and TAPS IP Phone Addition, on page 41

Cisco Unified Communications Manager Administration Conference Station Addition, on page 41

Conference Phone MAC Address Determination, on page 42

# Conference Phone MAC Address Determination

Several procedures described in this manual require you to determine the MAC address of a conference phone. You can determine the MAC address for a conference phone in any of these ways:

- From the conference phone, press **Apps**, select **Phone Information**, and look at the MAC Address field.
- Look at the MAC label on the bottom of the conference phone.
- Display the web page for the conference phone web page, and select **Device Information**. For information about accessing the conference phone web page, see Access Web Page, on page 112.

CHAPTER 5

# Cisco Unified IP Conference Phone Installation

## Cisco Unified IP Conference Phone Installation Overview

This chapter helps you set up and install the Cisco Unified IP Conference Phone on an IP telephony network.

**Note** Before you install a conference phone, you must decide how to configure the conference phone in your network. After you have determined your configuration requirements, you can install the conference phone and verify its functionality. For more information, see Cisco Unified IP Phones and Telephony Networks, on page 33

## Before You Begin

Before you install the conference phone, review the requirements in the following sections.

### Network Requirements

For the Cisco Unified IP Conference Station to successfully operate as an endpoint in your network, your network must meet these requirements:

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

- IP network:
  - Support for Dynamic Host Configuration Protocol (DHCP) or manual assignment of IP address, gateway, and subnet mask

**Note** The conference phone displays the data and time from Cisco Unified Communications Manager. If the Cisco Unified Communications Manager server is located in a different time zone than the conference stations, the conference stations do no display the correct local time.

# Cisco Unified Communications Manager Setup

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

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

You must use Cisco Unified Communications Manager to configure and assign telephony features to the conference phones.

In Cisco Unified Communications Manager, you can add users to the database, add users to user groups, and associate users with specific conference phones. In this way, users gain access to Cisco Unified Communications Self Care Portal that allow them to configure items such as call forwarding and voice messaging system options.

### Related Topics

Cisco Unified Communications Manager IP Phone Addition Methods, on page 39

Available Telephony Features, on page 74

# Wireless Microphone Region Setting

The Wireless Microphone Frequency Lock feature provides a secure DECT frequency for wireless microphones by locking down the Wireless Region setting. The Cisco Unified IP Conference Phone 8831 is shipped from the manufacturer with the mask and the Wireless Region setting configured for your region.

The Cisco Unified IP Conference Phone 8831NR does not support wireless microphones.

For additional information, see *Cisco Unified IP Conference Phone 8831 Release Notes for Firmware Release 10.3(1)*.

# Safety

Review the following warnings before installing the conference station. To see translations of these warnings, see the Regulatory Compliance and Safety Information for Cisco Unified IP Conference Stations document that accompanied this device.

⚠ **Attention** Read the installation instructions before you connect the system to its power source.

⚠ **Attention** Only trained and qualified personnel should be allowed to install, replace, or service this equipment.

⚠ **Attention** Ultimate disposal of this product should be handled according to all national laws and regulations.

⚠ **Attention** Do not work on the system or connect or disconnect cables during periods of lightning activity.

⚠ **Caution** To avoid electric shock, do not connect safety extra low voltage (SELV) circuits to teleconference station network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Some LAN and WAN ports both use RJ-45 connectors. Use caution when connecting cables.

The following warnings apply when you use an external power supply.

⚠ **Attention** This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 15 A U.S. (240 VAC, 10 A international) is used on the phase conductors (all current-carrying conductors

⚠ **Attention** The device is designed to work with TN power systems.

⚠ **Attention** The plug-socket combination must be accessible at all times because it serves as the main disconnecting device.

# Cisco Unified IP Conference Phone Components

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

## Network Ports

The underside of the conference phone sound base has a single network port. This port is labeled LAN.

Your conference phone has a 10/100 Base-T autosensing Ethernet port. This port supports Mbps half- or full-duplex connections to external devices. You can use either Category 3 or 5, or 5e cabling for 10-Mbps connections, but you must use Category 5 or 5e for 100 Mbps connections.

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

**Related Topics**

Conference Phone Power, on page 35

Phone Connections, on page 48

# Wired Extension Microphone Kit

The optional wired extension microphone kit includes two wired omni-directional microphones. Connecting a microphone kit enhances the room coverage of the conference phone. The sound base has two wired microphone ports and you can connect one or both wired microphones.

If the conference phone is connected to another sound base in Linked Mode, the primary base station supports one or two wireless microphones, or it supports one wired microphone. The secondary unit supports only one wired microphone; a wireless microphone cannot be connected to a secondary Sound Base. You cannot mix microphone kits: if you plan to connect a microphone to both sound bases, they must both be wired microphones.

**Note** Wired and wireless microphones cannot be used at the same time, and the wireless microphones have a higher priority. Attempting to connect a wired microphone to a conference phone that has paired or connected channels results in a warning to the user that the wired microphone is disabled. To solve this problem, unpair any paired or connected wireless microphones before connecting a wired microphone.

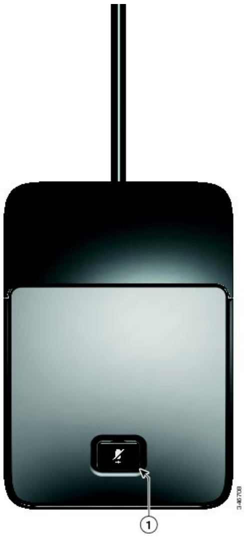


*Table 16: Wired Microphone Buttons*

| Item | Description |
|---|---|
| 1 | Mute button. |

# Wireless Extension Microphone Kit

The optional wireless microphone extension kit enhances the room coverage of the conference phone. Two wireless microphones can be paired to the conference phone.

The Cisco Unified IP Conference Phone 8831NR does not support wireless microphones.

Wireless microphones support an 8-hour call before the battery requires charging. The charger is separate device, and is not connected to the conference phone.

LEDs on the wireless microphone base indicate the connection status of the microphone, and an icon will also be displayed on the conference phone screen. The LEDs and the display screen also indicate the mute status of the wireless microphone.

If your conference phone is to be configured to use wireless extension microphones, you can access the configuration menu from the conference phone by choosing **Apps** > **Admin Settings** > **Wireless Microphones**. From this menu, the user can choose which channel to set in pairing mode, initiate the pairing process, and set the wireless microphone range.

The wireless microphone range is used to set the baseband power and effective RF range for the wireless microphones. There are three possible setting for the wireless microphone range:

- Low
- Medium
- High

If the conference phone is connected to another sound base in Linked Mode, the primary base station supports one or two wireless microphones, or it supports one wired microphone. The secondary unit supports only one wired microphone; a wireless microphone cannot be connected to a secondary Sound Base. You cannot mix microphone kits: if you plan to connect a microphone to both sound bases, they must both be wired microphones.

**Note** Wired and wireless microphones cannot be used at the same time, and the wireless microphones have a higher priority. Attempting to connect a wired microphone to a conference phone that has paired or connected channels results in a warning to the user that the wired microphone is disabled. To solve this problem, unpair any paired or connected wireless microphones before connecting a wired microphone.

### Related Topics

Wired Extension Microphone Kit, on page 46
Wireless Microphone Menu, on page 51
Unpair Wireless Microphone, on page 53
Pair Wireless Microphone, on page 52

# Cisco Unified IP Conference Phone Setup

You must connect the Cisco Unified IP Conference Phone to the network and to a power source before using it.

**Note** Before connecting the ethernet cable to the device, you must first install a ferrite bead on the ethernet cable.

**Note** Before you install a conference phone or phone, even if it is new, upgrade the device to the current firmware image. Before using external devices, see the Readme file for safety and performance information.

See Buttons and Hardware, on page 10 for a diagram of the connections for the Cisco Unified IP Conference Phone.

### Related Topics

Install Ferrite Bead on Network Cable, on page 49

# Phone Connections

The Sound Base contains the network and power connection for the phone. The base also contains the mini-USB connection for the DCS, the wired microphone ports, and the daisy chain port for the Linked Mode feature.

You can use the graphic and table below to identify connections and ports on the Sound Base.

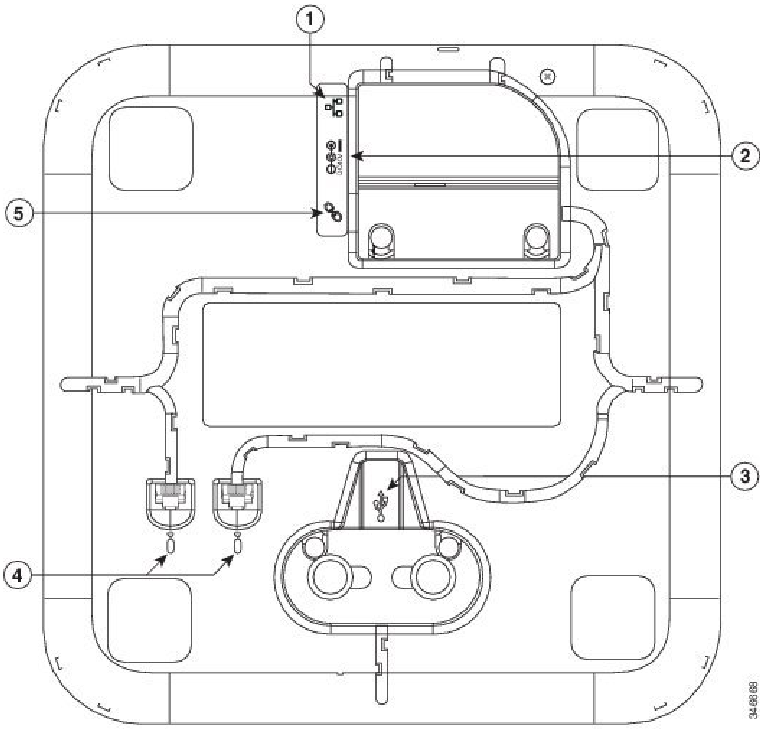


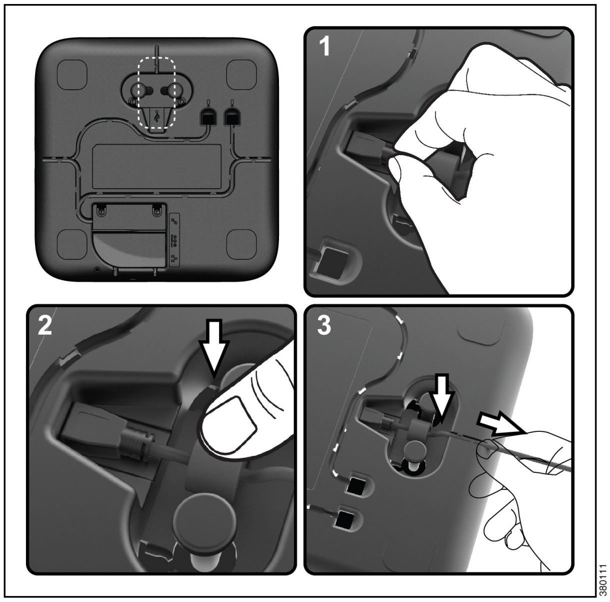
*Table 17: Sound Base Connections and Ports*

| | Item | Description |
|---|---|---|
| 1 | Network port | Network port (10/100 SW) connection. IEEE 802.3af power enabled. |

| | Item | Description |
|---|---|---|
| 2 | Wall power | Local power connection. |
| 3 | Mini USB port | Connects the base station to the DCU.<br>**Attention** When connecting the USB cable, firmly press down on the ferrite bead to ensure it seats correctly between the posts. |
| 4 | Wired microphone ports | Two RJ11 microphone ports. An optional wired microphone can be connected to each port. |
| 5 | Linked Mode daisy chain port | Supports the connection of two base stations in Linked Mode. |

## Connect Mini-USB Cable to DCU

The following images show how to install the USB cable.



### Procedure

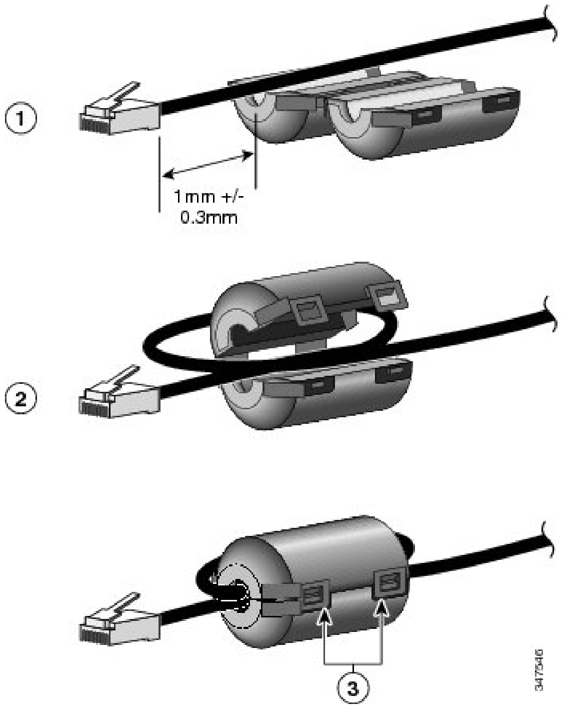
**Step 1** Insert the mini-USB connector into the port on the base of the phone.

**Step 2** Seat the ferrite bead between the posts and press the bead down firmly.

**Step 3** Thread the cable in the cable channel. Make sure that you leave some slack in the cable.

## Install Ferrite Bead on Network Cable

The following images show how to install the ferrite bead on the network cable.



**Procedure**

**Step 1** Align the ferrite bead with the head of the network cable and move the ferrite bead along the cable until there is a gap of 1.0 mm +/- 0.3 mm between the bead and the connector.

**Step 2** Place the cable into the ferrite bead channel and loop the cable around the ferrite bead so that the cable exits the bottom of the bead.

**Step 3** Hold the cable in the ferrite bead channel and close the ferrite bead. Snap the latch closed.

# Install Cisco Unified IP Conference Phone

**Note** Before you install a conference phone, even if it is new, upgrade the conference phone to the current firmware image. Before using external devices, see the Readme file for safety and performance information.

**Procedure**

**Step 1** Connect the power supply to the Cisco DC Adapter port. See the Power Guidelines, on page 35 for more information about powering your conference phone.

**Step 2** Connect a straight-through Ethernet cable from the switch to the network port on the conference phone. Each Cisco Unified IP Conference Phone 8831 ships with one ethernet cable in the box.

You can use either Category 3, 5, or 5e cabling for 10-Mbps connections, but you must use Category 5 or 5e for 100 Mbps connections.

See Network Ports, on page 45 for guidelines.

**Step 3** (Optional) Connect wired extension microphones.

## Performance Guidelines

Follow these guidelines to ensure optimum performance with the conference phone and the wired or wireless extension microphones if they are connected.

- Use the conference phone in closed offices and conference rooms up to 20 feet by 20 feet (without external microphones) and 20 feet by 30 feet (with external microphones).
- Place the conference phone base on a flat surface and make sure that it is clear from any reflective surfaces.
- Maintain a minimum distance of four feet between each external microphone and the conference phone base and other objects.
- Make sure that all microphones are acoustically unobstructed.
- Position the external microphones toward the areas that need to be covered, and so that the main pickup direction is pointed away from the conference phone.
- Seat all conference participants the same distance from the conference phone.
- Speak at normal conversation levels and direct your voice toward the conference phone.
- Do not move or handle the conference phone base or the external microphones while on a call, and do not shuffle papers near the equipment.
- Minimize background noise from air conditioning units, fans, or other equipment in the office or conference room.

## Wireless Microphone Menu

The Wireless Microphone menu provides options for setting the pairing and range options for the wireless expansion microphones. A maximum of two wireless microphones can be paired with the conference station at a time.

The Cisco Unified IP Conference Phone 8831NR does not support wireless microphones.

To access the Wireless Microphone menu, navigate to **Apps** > **Admin Settings** > **Wireless Microphones**.

The following table describes the Wireless Microphone Options and, where applicable, explains how to change them.

*Table 18: Wireless Microphone Options*

| Option | Description | To Change |
|---|---|---|
| Wireless Microphone 1 | The channel that can be used to pair the first microphone. | See Pair Wireless Microphone, on page 52 or Unpair Wireless Microphone, on page 53 |
| Wireless Microphone 2 | The channel that can be used to pair the second microphone. | See Pair Wireless Microphone, on page 52 or Unpair Wireless Microphone, on page 53 |
| Wireless Microphone Range | Sets the baseband power and effective RF range for the wireless microphones.<br>The RF range can be set to<br>• Low<br>• Medium<br>• High | Select Low, Medium or High, and press **Select**. Or press **Default** to select the default setting and press **Select**. |

## Pair Wireless Microphone

### Before you begin

The microphone must be in the off state before you can pair it to the conference station. A microphone is off if the microphone's LED is off. To turn off the wireless microphone, hold down the microphone button until the microphone LED turns solid red, then release.

### Procedure

**Step 1** Choose **Apps** > **Admin Settings** > **Wireless Microphones**.

**Step 2** Select either Wireless Microphone 1 or Wireless Microphone 2.

If the selected channel is available, a `Pair microphone 1?` or `Pair microphone 2?` prompt displays, and the **Pair** softkey displays.

If a microphone is already linked to a particular channel, pairing cannot be initiated on the selected channel and the dialog shows that the microphone is linked.

**Step 3** Press **Pair**.

If the channel is ready to pair, the pairing process begins and a text message displays.

**Step 4** Put the microphone that corresponds to the selected channel in pairing mode by pressing the microphone's Mute button until the LED lights solid red.

If pairing succeeds, the screen reverts to the Wireless Microphones Menu, and the message `Mic X Paired Successfully!` displays.

If pairing times out or fails, the status is updated and you can cancel or retry.

**Step 5** Press **Cancel** to revert to the Wireless Microphones Menu.

**Step 6** Press **Retry** to start the pairing process again.

**Related Topics**

Unpair Wireless Microphone, on page 53

## Unpair Wireless Microphone

If you need to connect a wired microphone to the conference station, any wireless microphones must be unpaired first. You can also use this procedure to unpair a microphone that is no longer in use.

**Note** This option is not available if the microphone is connected. To enable the unpair command, place the wireless microphone in its charger or turn it off.

**Procedure**

**Step 1** Choose **Applications** > **Admin Settings** > **Wireless Microphones**.

**Step 2** Select either Wireless Microphone 1 or Wireless Microphone 2.

If the selected channel is paired, the **Unpair** softkey displays.

**Step 3** Press **Unpair**.

A verification prompt with the options to Cancel or **Unpair** displays.

**Step 4** Press **Unpair** to continue to unpair the microphone.

The microphone channel's registration information in the base deletes. If you view the microphone channel's status in phone info menu, the status value and RFID are empty.

**Step 5** Press return to revert to the wireless microphones menu and stop the process.

**Related Topics**

Pair Wireless Microphone, on page 52

# IP Phone Startup Verification

After the conference phone has power connected to it, it begins the startup diagnostic process by cycling through the following steps.

1. The specified LED buttons flash on and off during the various stages of boot up as the conference phone checks its hardware. See the following table for a list of the hardware test and the LED diagnostic status.

*Table 19: LED Diagnostic Status*

| Hardware Test | Sound Base LEDs | DCU LEDs |
|---|---|---|
| Power is Ready | Green LEDs flash | Red and Green LEDs flash |

| Hardware Test | Sound Base LEDs | DCU LEDs |
|---|---|---|
| Flash is Accessible | Green LEDs flash | Red and Green LEDs flash |
| RAM Test Successful | Green LEDs flash | Red and Green LEDs flash |
| Ethernet Test Successful | — | — |

2. The screen displays the Cisco Systems, Inc., logo screen.
3. The screen displays the Revolabs, Inc., splash screen
4. This message appears as the conference phone starts up.
    - `Phone is not registered`
5. The home screen displays:
    - Current date and time
    - Primary directory number
    - Softkeys

If the conference phone successfully passes through these stages, it has started up properly. If the conference phone does not start up properly, see Startup Problems, on page 121.

# Network Settings

If you are not using DHCP in your network, you must configure these network settings on the conference phone after installing it on the network:

- IP address
- IP subnet information (subnet mask)
- TFTP server IP address
- You also may configure the domain name and the DNS server settings, if necessary.

Collect this information before you start to configure the conference phone.

**Related Topics**

Cisco Unified IP Conference Phone Settings, on page 59

# Cisco Unified IP Phone Security

The security features protect against several threats, including threats to the identity of the conference phone and to data. These features establish and maintain secure communication streams between the conference phone and the Cisco Unified Communications Manager server, and digitally sign files before they are delivered.

For more information about the security features, see Cisco Unified IP Conference Phone Security Features, on page 20 and also consult the *Cisco Unified Communications Manager Security Guide*.

# Set Up Locally Significant Certificate

You can initiate the installation of a Locally Significant Certificate (LSC) from the Security Configuration menu on the conference phone. This menu also lets you update or remove an LSC.

To manually configure an LSC on the conference phone, perform these steps:

### Before you begin

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

- The CTL file should have a CAPF certificate.
- On Cisco Unified Communications Operating System Administration, verify that the CAPF certificate has been installed.
- The CAPF is running and configured.

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

### Procedure

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

**Step 2** From the phone, choose **Apps** > **Admin Settings** > **Security Configuration**.

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

**Step 3** Scroll to LSC and press **Update**.

The conference phone prompts for an authentication string.

**Step 4** Enter the authentication code and press **Submit**.

The conference phone begins to install, update, or remove the LSC, depending on how the CAPF was configured. During the procedure, a notification message is displayed so that you can monitor progress.

The LSC install, update, or removal process can take a long time to complete. You can stop the process at any time by pressing **Exit**.

You can verify that an LSC is installed on the conference phone by choosing **Apps** > **Admin Settings** > **Security Setup** and ensuring that the LSC setting shows `Installed`.

CHAPTER 6

# Self Care Portal Management

## Self Care Portal Overview

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

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

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

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

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

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

- A user ID and default password to access the application.

- An overview of the tasks that users can accomplish with the portal.

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

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

## Set Up User Access to the Self Care Portal

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

### Procedure

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

**Step 2** Search for the user.

**Step 3** Click the user ID link.

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

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

**Step 6** Select **Save**.

# Customize the Self Care Portal Display

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

- Show Ring Settings
- Show Line Label Settings

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

### Procedure

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

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

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

**Step 4** Select **Save**.

CHAPTER 7

# Cisco Unified IP Conference Phone Settings

## Cisco Unified IP Conference Phone Configuration Menus

The conference phone includes the following configuration menus:

- Network Setup: Provides options for viewing and for configuring network settings.
- IPv4 Configuration: A submenu of the Network Setup menu, the IPv4 menu items provide additional network options field that can be viewed or set.

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

You can control whether a conference phone user has access to conference phone settings by using the Settings Access field on the Phone Configuration page in Cisco Unified Communications Manager Administration. For more information, see the *Cisco Unified Communications Manager Administration Guide*.

### Related Topics

Network Setup Menu, on page 62

Security Setup Menu, on page 69

# Display the Configuration Menu

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

- **Enabled:** Allow access to the Settings menu.
- **Disabled:** Prevent access to the Settings menu.
- **Restricted:** Allow access to the User Preferences menu, but prevent access to other options on the Settings menu.

If you cannot access an option on the Administrator Settings menu, check the Settings Access field. For more information, see the *Cisco Unified Communications Manager Administration Guide*.

To display a configuration menu, perform these steps:

## Procedure

**Step 1** Press **Apps**.

**Step 2** Select **Admin Settings**.

**Note** For information about the Status menu, see Model Information, Status, and Statistics, on page 105. For information about the Reset Settings menu, see Troubleshooting and Maintenance, on page 121.

**Step 3** Enter the password and then press **Enter**. The Admin Settings password is configured in the Local Phone Unlock Password parameter in the Common Phone Profile Configuration on Cisco Unified Communications Manager Administration.

**Note** Users can access the Admin Settings without entering a password when the Local Phone Unlock Password parameter is not configured

**Step 4** Perform one of these actions to display the desired menu:

- Use the navigation bar 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 5** To display a submenu, repeat Step 4.

**Step 6** To exit a menu, press **Exit**.

### Related Topics

Value Input and Editing Guidelines, on page 61
Security Setup Menu, on page 69
Network Setup Menu, on page 62

# Password Protection

You can apply a password to the phone so that no changes can be made to the administrative options on the conference phone unless the password is entered on the Admin Settings phone screen.

## Apply Password

To apply a password to the conference 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** In the Local Phone Unlock Password option, enter a password.

**Step 3** Apply the password to the common phone profile used by the phone.

# Value Input and Editing Guidelines

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

- Use the keys on the keypad to enter numbers and letters.
- To enter letters by using the keypad, use the corresponding number key. Press the key one or more times to display a particular letter. For example, press **2** 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.
- To enter a period (for example, in an IP address), press * on the keypad.
- To enter a plus (+), for international dialling, press and hold the ***** key for at least 1 second.
- Press the up arrow on the navigation bar to move the cursor to the left most character, and press the down arrow on the navigation bar to move the cursor to the right most character.
- Press ⌫ 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 have made.

**Note** The Cisco Unified IP Conference Phone provides several methods you can use to reset or restore option settings, if necessary. For more information, see Reset or Restore.

**Related Topics**

Display the Configuration Menu, on page 60

# User Interface Menus

# Network Setup Menu

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

For information about how to access the Network Setup menu, see Display Configuration menu.

*Table 20: Network Setup Menu Options*

| Option | Description | To Change |
|---|---|---|
| IPv4 Setup | In the IPv4 Setup submenu, you can do the following:<br>• Enable or disable the phone to use the IP address that is assign by the DHCP server.<br>• Manually set the IP Address, Subnet Mask, Default Routers, DNS Server, and Alternate TFTP servers.<br>For more information on the IPv4 address fields, see IPv4 Setup Menu Items. | Scroll to IPv4 Setup and press **Select**. |
| Host Name | Unique host name that the DHCP server assigned to the phone. | Display only—Cannot configure. |
| Domain Name | Name of the Domain Name System (DNS) domain in which the phone resides. | See Set Domain Name, on page 63. |
| Operational VLAN ID | Auxiliary Virtual Local Area Network (VLAN) configured on a Cisco Catalyst switch in which the phone is a member.<br>If the phone has not received an auxiliary VLAN, this option indicates the Administrative VLAN.<br>If neither the auxiliary VLAN nor the Administrative VLAN are configured, this option defaults to a VLAN ID of 4095. | Display only—Cannot configure.<br>The phone obtains its Operational VLAN ID via Cisco Discovery Protocol (CDP) from the switch to which the phone is attached. To assign a VLAN ID manually, use the Admin VLAN ID option. |

| Option | Description | To Change |
|---|---|---|
| Admin. VLAN ID | Auxiliary VLAN in which the phone is a member.<br>Used only if the phone does not receive an auxiliary VLAN from the switch; otherwise it is ignored. | See Set Admin VLAN ID, on page 64. |
| Network (SW) Port Setup | Speed and duplex of the network port. Valid values:<br>• Auto Negotiate<br>• 100 Half: 100-BaseT/half duplex<br>• 100 Full: 100-BaseT/full duplex<br>• 10 Half: 10-BaseT/half duplex<br>• 10 Full: 10-BaseT/full duplex<br>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 auto-negotiate. | |

### Related Topics

Display the Configuration Menu, on page 60
Value Input and Editing Guidelines, on page 61

## Set Domain Name

### Procedure

**Step 1** Set the DHCP Enabled option to **No**.

**Step 2** Choose **Apps** > **Admin Settings** > **Network Configuration** > **Domain Name**.

**Step 3** Enter a new domain name.

**Step 4** Press **Validate**, and then press **Save**.

### Related Topics

Set DHCP, on page 65

## Set Admin VLAN ID

### Procedure

**Step 1** Choose **Apps** > **Admin Settings** > **Network Configuration** > **Admin VLAN ID**.

Enter your password at the prompt.

**Step 2** Enter a new Admin VLAN ID.

**Step 3** Press **Apply**, and then **Save**.

## IPv4 Setup Menu Options

The IPv4 Setup menu is a submenu of the Network Setup menu. To reach the IPv4 Setup menu, select the IPv4 option on the Network Setup menu.

The following table describes the IPv4 Setup menu options.

For information about the keys you can use to edit options, see Value Input and Editing Guidelines, on page 61.

*Table 21: IPv4 Setup Menu Options*

| Option | Description | To Change |
|---|---|---|
| DHCP | Indicates whether the conference phone has DHCP enabled or disabled.<br>When DHCP is enabled, the DHCP server assigns the conference phone an IP address. When DHCP is disabled, the administrator must manually assign an IP address to the phone.<br>For more information, see DHCP Usage, on page 68. | Set DHCP, on page 65 |
| IP Address | Internet Protocol (IP) address of the conference phone.<br>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. | Set IP Address, on page 66 |
| Subnet Mask | Subnet mask used by the phone. | Set Subnet Mask, on page 66 |

| Option | Description | To Change |
|---|---|---|
| Default Router 1 | Default router used by the phone (Default Router 1). | Set Default Router, on page 66 |
| DNS Server 1 | Primary Domain Name System (DNS) server (DNS Server 1) and optional backup DNS servers (DNS Server 2–5) used by the phone. | Set DNS Server, on page 67 |
| Alternate TFTP | Indicates whether the phone is using an alternative TFTP server. | Set Alternate TFTP, on page 67 |
| TFTP Server 1 | Primary Trivial File Transfer Protocol (TFTP) server used by the phone. If you are not using DHCP in your network and you want to change this server, you must use the TFTP Server 1 option.<br>If you set the Alternate TFTP option to yes, you must enter a nonzero value for the TFTP Server 1 option. | Set TFTP Server 1, on page 67 |
| TFTP Server 2 | Optional backup TFTP server that the phone uses if the primary TFTP server is unavailable. | Set TFTP Server 2, on page 68 |
| DHCP Address Released | Releases the IP address assigned by DHCP. | |

# Set DHCP

### Procedure

**Step 1** Unlock network configuration options.

**Step 2** Choose **Apps** > **Admin Settings** > **Network Configuration** > **DHCP Enabled**.

**Step 3** Set Enable to Yes. To disable DHCP, set Enable to No.

**Step 4** Press **Select**, and then press **Save**.

# Set IP Address

### Procedure

**Step 1** Set the DHCP Enabled option to **No**.

**Step 2** Choose **Apps** > **Admin Settings** > **Network Configuration** > **IP Address**.

**Step 3** Enter a new IP Address.

**Step 4** Press **Validate**, and then press **Save**.

# Set Subnet Mask

### Procedure

**Step 1** Set the DHCP Enabled option to **No**.

**Step 2** Choose **Apps** > **Admin Settings** > **Network Configuration** > **IP Subnet Mask**.

**Step 3** Enter a new IP address for the subnet mask.

**Step 4** Press **Validate**, and then press **Save**.

### Related Topics

Set DHCP, on page 65

# Set Default Router

### Procedure

**Step 1** Unlock network configuration options.

**Step 2** Set the DHCP Enable option to **No**.

**Step 3** Choose **Apps** > **Admin Settings** > **Network Configuration** > **Default Router1**.

**Step 4** Enter a new router IP address.

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

### Related Topics

Set DHCP, on page 65

# Set DNS Server

### Procedure

Step 1 Unlock network configuration options.

Step 2 Set the DHCP Enable option to No.

Step 3 Choose **Apps** > **Admin Settings** > **Network Configuration** > **DNS Server1**.

Step 4 Enter a new DNS server address.

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

Step 6 Repeat as needed to assign backup DNS servers

### Related Topics

Set DHCP, on page 65

# Set Alternate TFTP

### Procedure

Step 1 Choose **Apps** > **Admin Settings** > **Network Configuration** > **Alternate TFTP**.

Step 2 Press **Yes** if the conference station should use an alternate TFTP server, or **No** if the conference station should not use an alternate TFTP server.

Step 3 Press **Select**, and then press **Save**.

# Set TFTP Server 1

### Procedure

Step 1 If DHCP is enabled, set the Alternate TFTP option to **Yes**.

Step 2 Choose **Apps** > **Admin Settings** > **Network Configuration** > **TFTP Server 1**.

Step 3 Press **Edit**.

Step 4 Enter a new TFTP server IP address.

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

### Related Topics

Set DHCP, on page 65

# Set TFTP Server 2

**Procedure**

**Step 1** Choose **Apps** > **Admin Settings** > **Network Configuration** > **TFTP Server 1**.

**Step 2** Press **Edit** and enter an IP address for the TFTP Server 1 option.

**Step 3** Press **Apply**, and then press **Save**.

**Step 4** Choose **Apps** > **Admin Settings** > **Network Configuration** > **TFTP Server 2**.

**Step 5** Choose the TFTP Server 2 option, and then press **Edit**.

**Step 6** Enter a new backup TFTP server IP address.

**Step 7** Press **Apply**, and then press **Save**.

**Related Topics**

Set TFTP Server 1, on page 67

# DHCP Usage

Dynamic Host Configuration Protocol (DHCP) automatically assigns IP addresses to devices when you connect them to the network. Conference stations enable DHCP by default.

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 to assign it for you or by manually entering an IP address.

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

## Set Up IP 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 **Apps** and choose **Admin 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**, and then press **Save**.

## Set Up IP 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 conference station.

### Procedure

**Step 1** Press **Apps** and choose **Admin 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 the conference station.
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**, and then press **Save**.

### Related Topics

Set DHCP, on page 65
Set Subnet Mask, on page 66
Set IP Address, on page 66
Set Default Router, on page 66
Set Alternate TFTP, on page 67
Set TFTP Server 1, on page 67

# Security Setup Menu

The Security Setup menu provides information about various security settings. It provides access to the Trust List File screen and the 802.1x authentication.

Access the Security Configuration menu from **Apps** > **Admin Settings** > **Security Setup**

The following table describes the options in this menu.

*Table 22: Security Menu Settings*

| 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** > **Phone Configuration**. |

| Option | Description | To Change |
|---|---|---|
| LSC | Indicates if a locally significant certificate (used for the security features) is installed on the phone (Installed) or is not installed on the phone (Not Installed). | For information about how to manage the LSC for your phone, see "Using the Certificate Authority Proxy Function" chapter in *Cisco Unified Communications Manager Security Guide*. |
| Trust List | The Trust List provides submenus for CTL signature and Call Manager/TFTP Server. | For more information, see the Trust List Menu, on page 70. |
| 802.1X Authentication | Displays the device authentication, EAP/MD5, and transaction status. | See 802.1X Authentication and Status Menus, on page 71. |

**Related Topics**

Value Input and Editing Guidelines, on page 61

Display the Configuration Menu, on page 60

# Trust List Menu

The Trust List menu displays information about all the servers that the conference phone trusts, and includes the options described in the following table.

The Trust List is accessed via the **Apps** > **Admin Settings** > **Security Setup** > **Trust List**

To exit the Trust List Menu, press **Back**.

*Table 23: Trust List Menu Settings*

| Option | Description | To Change |
|---|---|---|
| CTL Signature | Displays the MD5 hash of the CTL file. | For more information about this file, see "Configuring the Cisco CTL Client" chapter in *Cisco Unified Communications Manager Security Guide*. |
| ITL File | Displays a submenu of options. Select an option to view its ITL setting information:<br>• ITL Signature: MD5 hash of the ITL file.<br>• Unified CM/TFTP Server<br>• CAPF Server<br>• TVS | For more information about this file, see "Configuring the Cisco ITL Client" chapter in the *Cisco Unified Communications Manager Security Guide*. |
| Call Manager/TFTP Server | Displays the call manager/TFTP certificate information. | |

# 802.1X Authentication and Status Menus

The 802.1X Authentication and 802.1X Authentication Status menus allow you to enable 802.1X authentication and view transaction status. These options are described in the following tables.

To exit these menus, press Exit.

*Table 24: 802.1X Authentication Settings*

| Option | Description | To Change |
|---|---|---|
| Device Authentication | Determines whether 802.1X authentication is enabled:<br>• Enabled: Phone uses 802.1X authentication to request network access.<br>• Disabled: Default setting in which the phone uses CDP to acquire VLAN and network access. | Set 802.1X Device Authentication, on page 72 |

*Table 25: 802.1X Authentication Status Setting*

| Option | Description | To Change |
|---|---|---|
| 802.1X Authentication Status | Real-time progress of the 802.1X authentication status, displaying one of the following states:<br>• Disabled: 802.1X is disabled and the transaction was not attempted<br>• Disconnected: Physical link is down or disconnected<br>• Connecting: Trying to discover or acquire the authenticator<br>• Acquired: Authenticator acquired, awaiting authentication to begin<br>• Authenticating: Authentication in progress<br>• Authenticated: Authentication successful or implicit authentication due to timeouts<br>• Held: Authentication failed, waiting before next attempt (approximately 60 seconds) | Display only—Cannot configure.<br>To view the transaction status of your 802.1X Authentication, choose **Applications** > **Admin Settings** > **Security Configuration** > **802.1X Authentication Status**. |

# Set 802.1X Device Authentication

### Procedure

**Step 1** ChooseApps > **Admin Settings** > **Security Config** > **802.1X Authentication** > **Device Authentication**.

**Step 2** Press **Edit**.

**Step 3** Set the Device Authentication option to **Enabled** or **Disabled**.

The default value is Disabled.

**Step 4** Press **Save**.

CHAPTER 8

# Features, Templates, Services, and User Setup

## Features, Templates, Services, and User Setup Overview

After you install conferences stations in your network, configure network settings, and add each Cisco Unified IP Conference Phone to Cisco Unified Communications Manager, you must use the Cisco Unified Communications Manager Administration application to configure telephony features, optionally modify conference 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 139.

For information about setting up conference phones in non-English environments, see International User Support, on page 143.

# Available Telephony Features

After you add Cisco Unified IP Conference Phones to Cisco Unified Communications Manager, you can add functionality. The following table includes a list of supported telephony features. You can use Cisco Unified Communications Manager Administration to configure many of these features. The Reference column lists Cisco Unified Communications Manager and other documentation that contains configuration procedures and related information.

For information about the use of these features on the phone, see the *Cisco Unified IP Conference Phone 8831 and 8831NR User Guide*.

**Note** Cisco Unified Communications Manager Administration also provides several service parameters that are used to configure various telephony functions. For more information about access and configuration of service parameters, see the *Cisco Unified Communications Manager Administration Guide*.

For more information on the functions of a service, select the name of the parameter or the question mark help button in the Service Parameter Configuration window in CUCM Administration.

*Table 26: Telephony Features for Cisco Unified IP Conference Phone 8831*

| 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 greetings as needed.<br>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**.<br>If Built In Bridge is set to Default, in the Cisco Unified Communications Manager Administration application, choose **System** > **Service Parameter** 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 the following:<br>• *Features and Services Guide for Cisco Unified Communications Manager*, “Barge and Privacy”<br>• *Cisco Unified Communications Manager System Guide*, “Cisco Unified IP Phones” |
| Any Call Pickup | Allows users to pick up a call on any line in their call pickup group, regardless of how the call was routed to the phone. | For more information, see *Features and Services Guide for Cisco Unified Communications Manager*, “Call Pickup” chapter. |

| Feature | Description | Configuration Reference |
|---|---|---|
| Audible Message Waiting Indicator (AMWI) | A stutter tone indicates that a user has one or more new voice messages on a line.<br>**Note** The stutter tone is line-specific. You hear it only when using the line with the waiting messages. | For more information, see *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones" chapter. |
| Auto Answer | Connects incoming calls automatically after a ring or two. | For more information, see *Cisco Unified Communications Manager Administration Guide*, "Directory Number Setup" chapter. |
| Auto Pickup | Allows a user to use one-touch pickup functionality for call pickup features. | For more information, see *Features and Services Guide for Cisco Unified Communications Manager*, "Call Pickup" chapter. |
| Block External to External Transfer | Prevents users from transferring an external call to another external number. | For more information, see *Features and Services Guide for Cisco Unified Communications Manager*, "External Call Transfer Restrictions" chapter. |
| Call Back | Provides users with an audio and visual alert on the phone when a busy or unavailable party becomes available. | For more information, see the following:<br>• *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones"<br>• *Features and Services Guide for Cisco Unified Communications Manager*, "Cisco Call Back" |
| Call Display Restrictions | Determines the information that will display for calling or connected lines, depending on the parties who are involved in the call. | For more information, see:<br>• *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Setup"<br>• *Cisco Unified Communications Manager System Guide*, "Understanding Route Plans"<br>• *Features and Services Guide for Cisco Unified Communications Manager*, "Call Display Restrictions" |

| Feature | Description | Configuration Reference |
|---|---|---|
| Call Forward | Allows users to redirect incoming calls to another number. Call Forward options include Call Forward All, Call Forward Busy, Call Forward No Answer, and Call Forward No Coverage. | For more information, see the following:<br>• *Cisco Unified Communications Manager Administration Guide*, “Directory Number Setup”<br>• *Cisco Unified Communications Manager System Guide*, “Cisco Unified IP Phones”<br>• Customize Cisco Unified Communications Manager Self Care Portal display |
| 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 Communications Manager System Guide*, “Cisco Unified IP Phones” chapter. |
| Call Forward All Loop Prevention | Prevents a user from configuring a Call Forward All destination directly on the phone that creates a Call Forward All loop or that creates a Call Forward All chain with more hops than the existing *Forward Maximum Hop* Count service parameter allows. | For more information, see *Cisco Unified Communications Manager System Guide*, “Cisco Unified IP Phones” chapter. |
| Call Forward Configurable Display | Allows you to specify information that appears on a phone when a call is forwarded. This information can include the caller name, caller number, redirected number, and original dialed number. | For more information, see the following:<br>• *Cisco Unified Communications Manager Administration Guide*, “Directory Number Setup”<br>• *Cisco Unified Communications Manager System Guide*, “Cisco Unified IP Phones” |
| 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 the *Cisco Unified Communications Manager System Guide*, “Directory Numbers” chapter. |
| Call Forward Notification | Allows you to configure the information that the user sees when receiving a forwarded call. | For more information, see Call Forward Notification setup. |
| Call History for Shared Line | Allows you to view shared line activity in the phone Call History. This feature will:<br>• Log missed calls for a shared line<br>• Log answered calls for a shared line | For more information, see Enable Call History for shared line. |

| Feature | Description | Configuration Reference |
|---|---|---|
| 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 the *Features and Services Guide for Cisco Unified Communications Manager*, "Call Park and Directed Call Park" chapter. |
| Call Pickup | Allows users to redirect a call that is ringing on another phone within their pickup group to their phone.<br>You can configure an audio and visual alert for the primary line on the phone. This alert notifies the users that a call is ringing in their pickup group. | For more information, see the *Features and Services Guide for Cisco Unified Communications Manager*, "Call Pickup" chapter. |
| 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.<br>When a call is secured, the security status of the call is displayed 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.<br>**Note** 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 will be 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 *Features and Services Guide for Cisco Unified Communications Manager*, "Monitoring and Recording" chapter. |
| Call Waiting | Indicates (and allows users to answer) an incoming call that rings while on another call. Incoming call information appears on the phone display. | For more information, see:<br>• *Cisco Unified Communications Manager System Guide*, "Directory Numbers"<br>• Phone Call Waiting setup |

| Feature | Description | Configuration Reference |
|---|---|---|
| Caller ID | Caller identification such as a phone number, name, or other descriptive text appear on the phone display. | For more information, see:<br>• *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Setup"<br>• *Cisco Unified Communications Manager System Guide*, "Understanding Route Plans"<br>• *Features and Services Guide for Cisco Unified Communications Manager*, "Call Display Restrictions"<br>• *Cisco Unified Communications Manager Administration Guide*, "Directory Number Setup" |
| Caller ID Blocking | Allows a user to block their phone number or email address from phones that have caller identification enabled. | For more information, see:<br>• *Cisco Unified Communications Manager System Guide*, "Understanding Route Plans"<br>• *Cisco Unified Communications Manager Administration Guide*, "Directory Number Setup" |
| Calling Party Normalization | Calling party normalization presents phone calls to the user with a dialable phone number. Any escape codes are added to the number so that the user can easily connect to the caller again. The dialable number is saved in the call history and can be saved in the Personal Address Book. | For more information, see Calling Party Normalization. |
| cBarge | Allows a user to join a nonprivate call on a shared phone line. cBarge adds a user to a call and converts it into a conference, allowing the user and other parties to access conference features | For more information, see:<br>• *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Setup"<br>• *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones"<br>• *Features and Services Guide for Cisco Unified Communications Manager*, "Barge and Privacy" |

| Feature | Description | Configuration Reference |
|---|---|---|
| Cisco Extension Mobility | Allows users to temporarily access their Cisco Unified IP Phone configuration such as line appearances and services from a shared Cisco Unified IP Phone by logging into the Cisco Extension Mobility service on that phone when they log into the Cisco Extension Mobility service on that phone.<br>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 “ Extension Mobility” chapter in the *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:<br>• Cisco Unified Communications Manager Express System Administrator Guide |
| Cisco WebDialer | Allows users to make calls from web and desktop applications. | For more information, see *Features and Services Guide for Cisco Unified Communications Manager*, “Web Dialer” chapter. |
| Conference | • Allows a user to talk simultaneously with multiple parties by calling each participant individually. Conference features include Conference and Meet Me.<br>• Allows a noninitiator in a standard (ad hoc) conference to add or remove participants; also allows any conference participant to join together two standard conferences on the same line. | The service parameter, Advance Adhoc Conference, (disabled by default in Cisco Unified Communications Manager Administration) allows you to enable these features.<br>For information on conferences, see *Cisco Unified Communications Manager System Guide*, “Conference Bridges” chapter.<br>For more information, see *Cisco Unified Communications Manager System Guide*, “Cisco Unified IP Phones” chapter.<br>**Note** Be sure to inform your users whether these features are activated. |
| 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 *Cisco Unified Communications Manager Administration Guide*, “CTI Route Point Setup” chapter. |

| Feature | Description | Configuration Reference |
|---|---|---|
| Device Invoked Recording | Provides end users with the ability to record their telephone calls via a softkey.<br>In addition administrators may continue to record telephone calls via the CTI User Interface. | For more information, see Enable Device Invoked Recording. |
| Directed Call Park | Allows a user to transfer an active call to an available directed call park number that the user dials.<br>**Note** If you implement Directed Call Park, avoid configuring the Park softkey. This prevents users from confusing the two Call Park features. | For more information, see *Features and Services Guide for Cisco Unified Communications Manager*, “Call Park and Directed Call Park” chapter. |
| Directed Call Pickup | Allows a user to answer a call that is ringing on a particular directory number. | For more information, see *Features and Services Guide for Cisco Unified Communications Manager*, “Call Pickup” chapter. |
| Direct Transfer | Allows users to connect two calls to each other without remaining on the line. | For more information, see *Cisco Unified Communications Manager System Guide*, “Cisco Unified IP Phones” chapter. |
| Distinctive Ring | Users can customize how their phone indicates an incoming call and a new voice mail message. | For more information, see *Features and Services Guide for Cisco Unified Communications Manager*, “Call Pickup” chapter. |
| Divert | Allows a user to transfer a ringing, connected, or held call directly to a voice-messaging system. When a call is diverted, the line becomes available to make or receive new calls. | For more information, see *Features and Services Guide for Cisco Unified Communications Manager*, “Immediate Divert” chapter. |

| 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.<br>The following DND-related parameters are configurable in Cisco Unified Communications Manager Administration:<br>• Do Not Disturb: This check box allows you to enable DND on a per-phone basis. Use **Cisco Unified Communications Manager Administration** > **Device** > **Phone** > **Phone Configuration**.<br>• DND Incoming Call Alert: Choose the type of alert to play, if any, on a phone for incoming calls when DND is active. This parameter is located on both the Common Phone Profile page and the Phone configuration page (Phone Configuration window value takes precedence). | For more information, see *Features and Services Guide for Cisco Unified Communications Manager*, “Do Not Disturb” chapter. |
| 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. |
| Enhanced Room Coverage | Optional microphone extension kits provide enhanced room coverage that can be further expanded by linking two units together in Linked Mode. | For more information see:<br>• *Cisco Unified IP Conference Phone 8831 User Guide for Cisco Unified Communication Manager*, “Conference Phone Link Mode” chapter.<br>• *Cisco Unified IP Conference Phone 8831 User Guide for Cisco Unified Communication Manager*, “Enhanced Room Coverage” chapter. |
| Fast Dial Service | Allows a user to enter a Fast Dial code to place a call. Fast Dial codes can be assigned to phone numbers or Personal Address Book entries. (See “Services” in this table.) | For more information, see Modify phone button template for PAB or Fast Dial. |
| Group Call Pickup | Allows a user to answer a call that is ringing on a directory number in another group. | For more information, see *Features and Services Guide for Cisco Unified Communications Manager*, “Call Pickup” chapter. |

| Feature | Description | Configuration Reference |
|---|---|---|
| Hold Reversion | Limits the amount of time that a call can be on hold before reverting back to the phone that put the call on hold and alerting the user.<br>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 not resumed.<br>A call that triggers Hold Reversion also displays an animated icon in the call bubble.<br>You can configure call focus priority to favor incoming or reverting calls. | For more information about configuring this feature, see *Features and Services Guide for Cisco Unified Communications Manager*, “Hold Reversion” chapter. |
| Hold Status | Enables phones with a shared line to distinguish between the local and remote lines that placed a call on hold. | No configuration is required. |
| Hold/Resume | Allows the user to move a connected call from an active state to a held state. | • Requires no configuration, unless you want to use Music On Hold. See “Music On Hold” in this table for information.<br>• See “Hold Reversion” in this table. |
| HTTP Download | Enhances the file download process to the phone to use HTTP by default. If the HTTP download fails, the phone reverts to using the TFTP download. | No configuration is required. |
| Jitter Buffer | The Jitter Buffer feature handles jitter from 10 milliseconds (ms) to 1000 ms for both audio and video streams. | No configuration required. |
| Linked Mode | Enhances the audio coverage area by using a daisy cable to connect two conference phone Sound Base units.<br>When linked, voice, dial tone, ringer and base LED features are synchronized between the two devices. | For more information see:<br>• *Cisco Unified IP Conference Phone 8831 User Guide*, “Conference Phone Link Mode” |
| Malicious Caller Identification (MCID) | Allows users to notify the system administrator about suspicious calls that are received. | For more information, see:<br>• *Cisco Unified Communications Manager System Guide*, “Cisco Unified IP Phones”<br>• *Features and Services Guide for Cisco Unified Communications Manager*, “Malicious Call Identification” |
| Meet Me Conference | Allows a user to host a Meet Me conference in which other participants call a predetermined number at a scheduled time. | For more information, see *Cisco Unified Communications Manager Administration Guide*, “Meet-Me Number and Pattern Setup” chapter. |

| Feature | Description | Configuration Reference |
|---|---|---|
| Message Waiting | Defines directory numbers for message waiting on and off indicators. A directly-connected voice-message 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 the following:<br>• *Cisco Unified Communications Manager Administration Guide*, "Message Waiting Setup"<br>• *Cisco Unified Communications Manager System Guide*, "Voice Mail Connectivity to Cisco Unified Communications Manager" |
| Message Waiting Indicator | Displays a New Voicemail status message on the phone screen. | For more information see:<br>• *Cisco Unified Communications Manager Administration Guide*, "Message Waiting Setup"<br>• *Cisco Unified Communications Manager System Guide*, "Voice Mail Connectivity to Cisco Unified Communications Manager" |
| Missed Call Logging | Allows a user to specify whether missed calls will be logged in the missed calls directory for a given line appearance. | For more information, see *Cisco Unified Communications Manager Administration Guide*, "Directory Number Setup" chapter. |
| Mobile Connect | Enables users to manage business calls using a single phone number and pick up in-progress calls on the desk phone and a remote device such as a mobile phone. Users can restrict the group of callers according to phone number and time of day. | For more information, see *Features and Services Guide for Cisco Unified Communications Manager*, "Cisco Unified Mobility" chapter. |
| 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 *Features and Services Guide for Cisco Unified Communications Manager*, "Cisco Unified Mobility" chapter. |

| Feature | Description | Configuration Reference |
|---|---|---|
| Monitoring and Recording | Allows a supervisor to silently monitor an active call. The supervisor cannot be heard by either party on the call. The user might hear a monitoring audible alert tone during a call when it is being monitored.<br>When a call is secured, the security status of the call is displayed 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 monitored.<br>**Note** When an active call is being monitored or recorded, the use can receive or place intercom calls; however, if the user place an intercom call, the active call will be 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 *Features and Services Guide for Cisco Unified Communications Manager*, "Monitoring and Recording" chapter. |
| Mute | Mutes the conference phone from the Sound Base, DCU or connected external microphones. | Requires no configuration. |
| No Alert Name | Makes it easier for end users to identify transferred calls by displaying the original caller's phone number. The call appears as an Alert Call followed by the caller's telephone number. | Requires no configuration. |
| Onhook Dialing | Allows a user to dial a number without going off hook. | For more information, see *Cisco Unified IP Conference Phone 8831 User Guide*. |
| Other Group Pickup | Allows a user to answer a call ringing on a phone in another group that is associated with the user's group. | For more information, see *Features and Services Guide for Cisco Unified Communications Manager*, "Call Pickup" chapter. |
| Phone Display Message for Extension Mobility Users | This feature enhances the phone interface for the Extension Mobility user by providing friendly messages. | No configuration required. |
| Plus Dialing | Allows the user to dial E.164 numbers prefixed with a plus (+) sign.<br>To dial the + sign, the user needs to press and hold the star (*) key for at least 1 second. This applies to dialing the first digit for an on-hook (including edit mode) or off-hook call. | No configuration required. |

| Feature | Description | Configuration Reference |
|---|---|---|
| Privacy | Prevents users who share a line from adding themselves to a call and from viewing information on their phone display about the call of the other user. | For more information, see the following:<br>• *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Setup"<br>• *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones"<br>• *Features and Services Guide for Cisco Unified Communications Manager*, "Barge and Privacy" |
| Quality Reporting Tool (QRT) | Allows users to submit information about problem phone calls by pressing a button. QRT can be configured for either of two user modes, depending upon the amount of user interaction desired with QRT. | For more information, see:<br>• *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones"<br>• *Features and Services Guide for Cisco Unified Communications Manager*, "Quality Report Tool" |
| Recording Tone | Indicates if a recording tone is enabled for the phone. | For more information, see Recording Tone, on page 92 |
| Redial | Allows users to call the most recently dialed phone number by pressing a button or the Redial softkey. | Requires no configuration. |
| Reroute Direct Calls to Remote Destination to Enterprise Number | Reroutes a direct call to a user's mobile phone to the enterprise number (desk phone). For an incoming call to remote destination (mobile phone), only remote destination rings; desk phone does not ring. When the call is answered on their mobile phone, the desk phone displays a Remote In Use message. During these calls, users can make use of various features of their mobile phone. | For more information, see the *Features and Services Guide for Cisco Unified Communications Manager*, "Cisco Unified Mobility" chapter. |

| 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 enhances the performance for large deployments with specific port settings.<br>**Note** If the ports are configured for Remote Port Configuration in Cisco Unified Communications Manager, the data cannot be changed on the phone. | To configure the parameter in the Cisco Unified Communications Manager Administration application, choose **Device** > **Phone**, select the appropriate IP phone, and scroll to the Product Specific Configuration Layout pane (Switch Port Remote Configuration or PC Port Remote Configuration).<br>To configure the setting on multiple phones simultaneously, configure the remote configuration in either Enterprise Phone Configuration (**System** > **Enterprise Phone Configuration**) or Common Phone Profile Configuration (**Device** > **Device Settings** > **Common Phone Profile**. (Switch Port Remote Configuration or PC Port Remote Configuration.) |
| Ringtone Setting | Identifies ring type used for a line when a phone has another active call. | For more information, see the following:<br>• *Cisco Unified Communications Manager Administration Guide*, “Directory Number Setup”<br>• *Cisco Unified Communications Manager Administration Guide*, “Custom Phone Rings” |
| Secure Conference | • Allows secure phones to place conference calls using a secured conference bridge.<br>• As new participants are added by using Conf, Join, cBarge, Barge softkeys or MeetMe conferencing, the secure call icon displays as long as all participants use secure phones.<br>• The Conference List displays the security level of each conference participant. Initiators can remove nonsecure participants from the Conference List. (Non-initiators can add or remove conference participants if the Advanced Adhoc Conference Enabled parameter is set.) | For more information about security, see Supported Security Features.<br>For additional information, see the following:<br>• *Cisco Unified Communications Manager System Guide*, “Conference Bridges”<br>• *Cisco Unified Communications Manager Administration Guide*, “Conference Bridge Setup”<br>• *Cisco Unified Communications Manager Security Guide* |
| Services | Allows you to use the Cisco Unified IP Phone Services Configuration menu in Cisco Unified Communications Manager Administration to define and maintain the list of phone services to which users can subscribe. | For more information refer to:<br>• *Cisco Unified Communications Manager Administration Guide*, “Cisco Unified IP Phone Setup”<br>• *Cisco Unified Communications Manager System Guide*, “Cisco Unified IP Phone Services” |

| Feature | Description | Configuration Reference |
|---|---|---|
| Shared Line | Allows a user to have multiple phones that share the same phone number or allows a user to share a phone number with a coworker. | For more information, see *Cisco Unified Communications Manager System Guide*, “Directory Numbers” chapter. |
| Special Sequence for Factory Reset | Allows the phone manufacturer to reset the factory parameters. | No configuration required. |
| Time-of-Day Routing | Restricts access to specified telephony features by time period. | For more information, see:<br>• *Cisco Unified Communications Manager Administration Guide*, “Time Period Setup”<br>• *Cisco Unified Communications Manager System Guide*, “Time-of-Day Routing” |
| Time Zone Update | Updates the Cisco Unified IP Phone with time zone changes. | For more information, see *Cisco Unified Communications Manager Administration Guide*, “Date and Time Group Setup” chapter. |
| TLS Enhancements | Added in Firmware Release 10.3(1)SR3.<br>Improved security with the parameter **Disable TLS1.0 and TLS1.1 for web access** in Cisco Unified Communications Manager. When set to enabled, the phones support only TLS1.2 mode. When set to disabled, TLS1.0, TLS1.1 and TLS1.2 are supported. This field applies to any phone or group of phones that function as a HTTPs server. | |
| Transfer | Allows users to redirect connected calls from their phones to another number. | Some JTAPI/TAPI applications are not compatible with the Join and Direct Transfer feature implementation on the conference phone and you may need to configure the Join and Direct Transfer Policy to disable join and direct transfer on the same line or possibly across lines. |
| Transfer - Direct Transfer | Transfer: The first invocation of Transfer will always initiate a new call by using the same directory number, after putting the active call on hold.<br>Direct Transfer: This transfer joins two established calls (call is in hold or in connected state) into one call and drops the feature initiator from the call. Direct Transfer does not initiate a consultation call and does not put the active call on hold. | Some JTAPI/TAPI applications are not compatible with the Join and Direct Transfer feature implementation on the conference phone and you may need to configure the Join and Direct Transfer Policy to disable join and direct transfer on the same line or possibly across lines. For more information, see the <xref Join and Direct Transfer Policy>. |

| Feature | Description | Configuration Reference |
|---|---|---|
| UCR 2008 | The conference phone supports Unified Capabilities Requirements (UCR) 2008 by providing support for 80-bit SRTCP Tagging.<br>As an administrator, you must set up specific parameters in Cisco Unified Communications Manager Administration. | See UCR 2008 setup. |
| Voice Message System | Enables callers to leave messages if calls are unanswered. | For more information, see the following:<br>• *Cisco Unified Communications Manager Administration Guide*, “Cisco Voice-Mail Port Setup”<br>• *Cisco Unified Communications Manager System Guide*, “Voice Mail Connectivity to Cisco Unified Communications Manager” |
| Wideband Ringtone | The Wideband Ringtone feature supports 10 ringtones: 4 embedded in the phone firmware and 6 downloaded from the Cisco Unified Communications Manager. | For more information, see the following:<br>• *Cisco Unified Communications Manager Administration Guide*, “Directory Number Setup”<br>• *Features and Services Guide for Cisco Unified Communications Manager*, “Custom Phone Rings” |
| Wireless Microphone Frequency Lock | Provides a secure DECT frequency for wireless microphones by locking down the Wireless Region setting. | No configuration required for Firmware release 10.3(1) and later. Earlier releases must upgrade to the current release to have the region setting locked.<br>**Note** Once you have configured the Wireless Region setting, it cannot be updated. Further configuration of this setting requires an RMA. |

# Corporate and Personal Directory Setup

The **Contacts** softkey on the conference phone gives users access to directory features. These directories can include:

- Corporate Directory: Supports a global corporate directory that users can access on the conference phone to lookup phone numbers of coworkers. You must enable and configure the corporate directories before they can be used.

- Personal Directory: Supports a personal address book (PAB) that allows a user to store a set of personal numbers. You must enable the feature and provide the user with a PIN and User ID to configure the features.

## 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 a user's right to access the system. Authorization identifies the telephony resources that a user is permitted to use, such as a specific teleconference phone extension.

To install and set up these features, see *Installing and Configuring the Cisco Customer Directory Configuration Plugin*. This document guides you through the configuration process for integrating Cisco Unified Communications Manager with Microsoft Active Directory and Netscape Directory Server. For more information, see "Understanding Directory Numbers" in the *Cisco Unified Communications Manager System Guide*.

After the LDAP directory configuration is complete, users can access the Corporate Directory service on the conference phone to find co-workers in the corporate directory.

## Personal Directory Setup

Personal Directory consists of the following features:

- Personal Address Book (PAB)
- Personal Fast Dials (Fast Dials)

Users can access Personal Directory features by these methods:

- From a web browser: Users can access the PAB from Cisco Unified Communications Manager Self Care Portal.
- From the conference phone: Users can choose **Contacts** > **Personal Directory** to access the PAB and Fast Dials features from their conference phones.

To configure Personal Directory from a web browser, users must access Cisco Unified Communications Manager Self Care Portal. You must provide users with a URL and login information.

# Button Templates

Using Cisco Unified Communications Manager Administration, you can assign button templates to conference phones. Cisco Unified Communications Manager contains the Standard 8831 button template for the Cisco Unified IP Conference Phone 8831 and 8831NR. When you assign the Standard 8831 button template to a conference phone, no buttons are added, but the **Privacy** softkey can be enabled from this template.

If the button feature is not configurable using the Button Template it may be a softkey feature that is configurable using a softkey template. For more information on softkey templates, see Softkey Templates, on page 90.

For more information on button templates, see the *Cisco Unified Communications Manager Administration Guide* and *Cisco Unified Communications Manager System Guide*.

## Add Phone Button Template

To add a button template,

### Procedure

**Step 1** Log on to Cisco Unified Communications Manager Administration.

**Step 2** Select **Device** > **Device Settings** > **Phone Button Template**.

**Step 3** Select **Add New**.

**Step 4** To assign a button template to a conference phone, choose **Device** > **Phone** to select the conference phone.

**Step 5** In the Phone Configuration window, select a button template from the Phone Button Template drop-down list.

# Softkey Templates

Using Cisco Unified Communications Manager Administration, you can manage softkeys associated with applications that are supported by the conference phone. Cisco Unified Communications Manager supports the Standard User and Standard Feature softkey templates.

An application that supports softkeys can have one or more standard softkey templates associated with it. You can modify a standard softkey template by making a copy of it, giving it a new name, and making updates to that copied softkey template. You can also modify a nonstandard softkey template.

To configure softkey templates, select **Device** > **Device Settings** > **Softkey Template** from Cisco Unified Communications Manager Administration. To assign a softkey template to a conference phone, use the Softkey Template field in the Cisco Unified Communications Manager Administration Phone Configuration page.

The Cisco Unified IP Conference Phone does not support all the softkeys that are configurable in Softkey Template Configuration on Cisco Unified Communications Manager Administration. The following table lists the features and softkeys that can be configured on a softkey template, and note whether it is supported on the conference phone.

**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 27: Configurable Softkeys*

| Feature | Configurable Softkeys in the Softkey Template Configuration | Supported as a Softkey | Notes |
|---|---|---|---|
| Answer | Answer (Answer) | Yes | — |

| Feature | Configurable Softkeys in the Softkey Template Configuration | Supported as a Softkey | Notes |
|---|---|---|---|
| Barge | Barge (Barge) | Yes | Configure as a softkey. |
| Call Back | Call Back (CallBack) | Yes | — |
| Call Forward All | Forward All (cfwdAll) | Yes | Phone displays **Fwd ALL** or **Fwd Off**. |
| Call Park | Call Park (Park) | Yes | — |
| Call Pickup | Pick Up (Pickup) | Yes | Configure as a softkey. |
| cBarge | Conference Barge (cBarge) | Yes | Configure as a softkey. |
| Conference | Conference (Conf) | Yes | Phone displays **Conference** when a call is connected. |
| Conference List | Conference List (ConfList) | Yes | Phone displays **ConfList** when in a conference. |
| iDivert | Immediate Divert (iDivert) | Yes | Phone displays **Divert**. |
| Do Not Disturb | Toggle Do Not Disturb (DND) | Yes | Configure as a softkey. |
| End Call | End Call (EndCall) | Yes | Phone displays **Cancel** if the call is not answered. |
| Group Pickup | Group Pick Up (GPickUp) | Yes | Configure as a softkey. |
| Hold | Hold (Hold) | Yes | |
| Join | Join (Join) | No | — |
| Malicious Call Identification | Toggle Malicious Call Identification (MCID) | Yes | Configure Malicious Call Identification as a softkey. |
| Meet Me | Meet Me (MeetMe) | Yes | Configure as a softkey. |
| Mobile Connect | Mobility (Mobility) | Yes | Configure Mobile Connect as a softkey. |
| New Call | New Call (NewCall) | Yes | Phone displays **New Call**. |
| Other Pickup | Other Pickup (oPickup) | Yes | Configure as a softkey. |

| Feature | Configurable Softkeys in the Softkey Template Configuration | Supported as a Softkey | Notes |
|---|---|---|---|
| Quality Reporting Tool | Quality Reporting Tool (QRT) | Yes | Configure Quality Reporting Tool as a softkey. |
| Redial | Redial (Redial) | Yes | Phone displays **Redial** when Off Hook. |
| Remove Last Conference Participant | Remove Last Conference Participant (Remove) | Yes | Phone displays **Remove** when a participant is selected. |
| Resume | Resume (Resume) | Yes | — |
| Transfer | Transfer | Yes | Phone displays **Transfer** when a call is connected. |

For more information, see *Cisco Unified Communications Manager Administration Guide*, “Softkey Template Configuration” and the *Cisco Unified Communications Manager System Guide*, “Softkey Template”.

## Set Up Softkey Templates

### Procedure

**Step 1** Log on to Cisco Unified Communications Manager Administration.

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

**Step 3** To assign a softkey template to a conference station, choose **Device** > **Phone** to select the conference station.

**Step 4** In the Phone Configuration window, select a softkey template from the Softkey Template drop-down list.

# Recording Tone

The Recording Tone feature indicates whether a recording tone is enabled or disabled for the phone. If this feature is enabled, all parties on a call hear the tone being played, regardless of whether the call is recorded or not. The tone first sounds when a call is answered.

**Note** Other related parameters — the recording tone frequency (in hz), the duration of the beep tone, and the beep tone interval (how often the beep tone plays) — are defined on a per-Network Locale basis in the xml file that defines tones. This xml file is named tones.xml or g3-tones.xml.

*Table 28: Recording Tone Parameters*

| Parameter | Note |
|---|---|
| Recording Tone Local Volume | Indicates the volume for the recording tone that the local party receives, if the local party phone has the Recording Tone option enabled.<br>This setting applies for each listening device, including the handset, speakerphone, and headset.<br>Range: 0 percent (no tone) to 100 percent (same level as current volume setting on the phone). |
| Recording Tone Remote Volume | Indicates the volume for the recording tone that the remote party receives. The remote party is the party who is on a call with the party whose phone has the Recording Tone option enabled.<br>Range: 0 percent to 100 percent. (0 percent is -66 dBM and 100 percent is -3 dBM).<br>Default: 50 percent. |
| Recording Tone Duration | Indicates the length of time in milliseconds that the tone plays.<br>If the value is less than one third of the interval, this value overrides the default provided that the Network Locale provides.<br>Range: 0 to 3000<br>**Note** For some Network Locales that use a complex cadence, this setting applies only to the first recording tone. |

# Enable Recording Tone

### Before you begin

You must be familiar with the Recording Tone parameters before you enable this feature.

**Note** You may want to notify your users if you enable this option. The default setting is Disabled.

### Procedure

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

**Step 2** Select **Enable** from the pulldown menu In the Recording Tone section.

**Step 3** Enter a value between 0 and 100 per cent in the Recording Tone Local Volume field.

**Step 4** Enter a value between 0 and 100 per cent in the Recording Tone Remote Volume field.

**Step 5** Click **Save**.

# Enable Device Invoked Recording

Configure the Device Invoked Recording feature from Cisco Unified Communications Manager. To enable this feature, perform the following steps.

### Procedure

**Step 1** Set the Built In Bridge to **On**.

**Step 2** Set Privacy to **Off**.

**Step 3** Set Recording Option to **Selective Call Recording Enabled**.

**Step 4** Select the appropriate Recording Profile.

# Enable Call History for Shared Line

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

**Note** For the purposes of this procedure, all references to a phone, device, or IP Phone apply to the conference phone.

### Procedure

**Step 1** Go to Cisco Unified CM Administration and choose **Device** > **Phone**.

**Step 2** Find your conference phone in 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:

**a.** Device Configuration window settings

**b.** Common Phone Profile window settings

c. Enterprise Phone Configuration window settings

# Services Setup

You can give users access to Cisco Unified IP Phone Services on the Cisco Unified IP Conference Phone. These services comprise XML applications that enable the display of interactive content with text and graphics on the conference phone. Examples of services include local movie times, stock quotes, and weather reports. Users access any configured services from the **Apps** softkey on the conference phone.

Before a user can access any service:

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

Before you set up services, gather the URLs for the sites you want to set up, and verify that users can access those sites from your corporate IP telephony network.

To set up these services choose **Device** > **Device Settings** > **Phone Services** from Cisco Unified Communications Manager. For more information, see the *Cisco Unified Communications Manager Administration Guide* and *Cisco Unified Communications Manager System Guide*.

After you configure these services, verify that your users have access to Cisco Unified Communications Manager Self Care Portal, from which they can select and subscribe to configured services. See IP Phone Features User Subscription and Setup, on page 140 for a summary of the information that you must provide to end users.

**Note** To configure Cisco Extension Mobility services for users, see “Cisco Unified Mobility”, *Cisco Unified Communications Manager Features and Services Guide*

# Cisco Unified Communications Manager User Addition

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 Call Forwarding numbers.
- Subscribe to services that are accessible from a Cisco Unified IP Phone.

You can add users to Cisco Unified Communications Manager using either of these methods:

- To add users individually, choose **User Management** > **End User** from Cisco Unified Communications Manager Administration.

  For more information on adding users, see the *Cisco Unified Communications Manager Administration Guide*. For details on user information, see the *Cisco Unified Communications Manager System 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 *Cisco Unified Communications Manager Bulk Administration Guide*.

- To add users from your corporate LDAP directory, choose **System** > **LDAP** > **LDAP System** from Cisco Unified Communications Manager Administration.

  **Note** After the Enable Synchronization from LDAP Server is enabled, you will not be able to add additional users from Cisco Unified Communications Manager Administration.

  For more information on LDAP, see the *Cisco Unified Communications Manager System Guide*, “Understanding the Directory”.

- To add a user and a phone at the same time, choose **User Management** > **User/Phone Add** from Cisco Unified Communications Manager.

# Call Waiting Setup

The Cisco Unified IP Conference Phone supports six calls on a single line. With multiple calls per line, setting up call waiting is simplified on the Cisco Unified Communications Manager. For more information, see “Understanding Directory Numbers”, *Cisco Unified Communications Manager System Guide*.

# Call Forward Notification Setup

You set up the information that is displayed to the user from within Cisco Unified Communications Manager Administration in the Device Configuration window (**Device** > **Phone** > **Line** > **Forwarded Call Information Display on Device**).

The following table describes the Call Forward Notification fields.

*Table 29: Call Forward Notification Fields*

| Field | Description | Default Checkbox State |
|---|---|---|
| Caller Name | When this check box is checked, the caller name displays in the notification window. | Checked |
| Caller Number | When this check box is checked, the caller number displays in the notification window. | Not checked |

| Field | Description | Default Checkbox State |
|---|---|---|
| Redirected Number | When this check box is checked, the information about the caller who last forwarded the call displays in the notification window.<br>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. | Not checked |
| Dialed Number | When this check box is checked, the information about the original recipient of the call displays in the notification window.<br>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. | Checked |

# Calling Party Normalization

In line with E.164 standards, calling party normalization enhances the dialing capabilities of some phones and improves call back functionality when a call is routed to multiple geographical locations. That is, the feature ensures that the called party can return a call without having to modify the directory number in the call log directories on the phone. Additionally, calling party normalization allows the user to globalize and localize phone numbers, so the appropriate calling number presentation displays on the phone.

The conference phone supports the following functions:

- For the final presentation of the calling number to the user, the conference phone screen displays the calling number based on the international, national, or local subscriber numbers.
    - If the call is an intra-city call, the calling number presented on the conference phone is displayed in the subscriber number format (without the area or city code).
    - For intercity calls, the calling number is presented in a national number format.
    - If the call is an international call, the calling number is presented with the E.164 format, with the plus (+) prefix digit.
- The call logs directories record the calling number in the received and missed call logs with the appropriate escape codes (9/0, 0/1, +). The user can go into directories, and select and dial one of these entries with the escape code without having to edit the number.

Configuring calling party normalization alleviates issues with toll bypass where the call is routed to multiple locations over the IP WAN. In addition, it allows Cisco Unified Communications Manager to distinguish the origin of the call to globalize or localize the calling party number for the conference phone user.

The conference phone itself can localize the calling party number. For the phone to localize the calling party number, you must configure the Calling Party Transformation CSS or the Use Device Pool Device Calling Party Transformation CSS setting in the Phone Configuration window.

Depending on your configuration for globalizing and localizing the calling party number, the phone user may see a localized number, a globalized number with access codes and prefixes, or the international escape character, +, in the calling party number. If a phone supports calling party normalization, the phone can show the localized calling party number on the conference phone screen and the globalized number in the call log directories on the conference phone.

In addition, these devices show both the globalized and localized calling party number in the Call Details. If a conference phone does not support calling party normalization, the device shows the localized calling party on the conference phone screen and in the call log directories on the phone.

For information on how to configure this feature for your conference phone, see “Calling Party Normalization”, *Cisco Unified Communications Manager Features and Services Guide*.

# Incoming Call Notification Window Timer Setup

You can set the time that the Incoming Call Notification Window, sometimes called a toast, displays on the conference 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 30: Incoming Call Notification Window Timer Field*

| Field | Description | Default Value |
|---|---|---|
| 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.<br>The possible values are 3, 4, 5, 6, 7, 8, 9, 10, 15, 30, and 60. | 5 seconds. |

# Linked Mode

Two conference phone Sound Base units can be linked together to expand the audio coverage area. One Sound Base acts as the primary device, and the other unit acts as the dependant or secondary device.

In Linked Mode, the primary base station supports either one wireless or one wired microphone. The secondary unit supports only one wired microphone. You cannot mix microphone kits: if you plan to connect a microphone to both sound bases, they must both be wired microphones.

The Cisco Unified IP Conference Phone 8831 supports wired and wireless microphones. The Cisco Unified IP Conference Phone 8831NR supports only wired microphones.

The voice, dial tone, ringer, and base LED features synchronize between the two devices when linked together. You can link two sound bases while a call is active.

When Linked Mode is active, the linked mode icon displays in the idle and the call screens.

The following table summarizes the best practice to follow when deploying your conference phones in Linked Mode. If the devices are linked in this manner, the system software automatically detects which device is to be used as the primary and which is the secondary one.

*Table 31: Linked Mode Setup Best Practice*

| Component | Connect to Primary | Connect to Secondary |
|---|---|---|
| Display Control Unit (DCU) | Yes | No |
| Network cable | Yes | No |
| Wall power | Yes | No |
| Optional Wired Microphone | Yes | Yes |
| Optional Wireless Microphone | Yes | No |

**Note** If a DCU is connected to the secondary device, it will display a prompt indicating that it is a dummy DCU, but will otherwise not function.

**Caution** When using a Sound Base in Linked Mode, the primary base unit must be connected using the CP-PWR-CUBE-3 external power supply.

If two devices are linked after both are registered, the user can select which is the primary device.

A secondary device receives upgrades to firmware seamlessly from the primary device.

# Link Conference Phones

Use a daisy cable to connect two sound base units in Linked mode. This procedure describes the best practice for connecting the two units.

### Procedure

**Step 1** Connect the DCU to the conference phone to be used as the primary unit.

**Step 2** Connect the network cable to the conference phone to be used as the primary unit.

**Step 3** Connect the power cable to the primary device and plug into a wall plug.

The secondary Sound Base does not need to be plugged into external power, but in Linked Mode the primary unit must be connected to external power.

**Step 4** Use the provided daisy cable to connect the primary unit to the secondary sound base.

Voice, dial tone, ringer and base LEDs synchronize between the two units.

### Related Topics

Linked Mode, on page 98

CHAPTER 9

# Cisco Unified IP Conference Phone Customization

## Cisco Unified IP Conference Phone Customization Overview

This chapter explains how you customize configuration files, Cisco Unified IP Conference Phone ring sounds, and the idle display at your site. Ring sounds play when the conference phone receives a call. The idle display appears on the LCD screen when the conference phone has not been used for a designated period.

## Configuration File Customization and Modification

You can modify configuration files and add customized files to the TFTP directory. You can modify files or add customized files to the TFTP directory in Cisco Unified Communications Operating System Administration, from the TFTP Server File Upload window. For information about how to upload files to the TFTP folder on a Cisco Unified Communications Manager server, see the *Cisco Unified Communications Manager System Guide*.

You can obtain a copy of the Ringlist.xml or Ringlist-wb.xml files and the List.xml file from the system using the following admin command-line interface (CLI) "file" commands:

- admin:file
  - file list
  - file view
  - file search
  - file get
  - file dump
  - file tail
  - file delete

For more information, see the *Cisco Intercompany Media Engine Command Line Interface Reference Guide*.

# Custom Phone Ring Creation

The default ringtone implemented in the conference phone hardware is Chirp1. Cisco Unified Communications Manager also provides a default set of additional conference phone ring sounds that are implemented in software as pulse code modulation (PCM) files. The PCM files, along with an XML file, `Ringlist-wb.xml`, which describe the ring list options that are available at your site, are found in the TFTP directory on each Cisco Unified Communications Manager.

Both file formats can be used simultaneously on the conference phone.

The conference phone ringtone formats are backward compatible with the G.711ulaw/8-bit/8000 Hz raw format as well as with previous Cisco Unified Communications Manager versions.

For more information, see the *Cisco Unified Communications Manager System Guide*, “Cisco TFTP” chapter, and *Cisco Unified Communications Operating System Administration Guide*, “Software Upgrades” chapter.

The following sections describe how you can customize the conference phone ringtones that are available at your site by creating PCM files and editing the Ringlist-wb.xml file.

## Ringlist-wb.xml File Format Requirements

The `Ringlist-wb.xml` file defines an XML object that contains a list of conference phone ring types. This file can include 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 will appear on the Ring Type menu on a conference phone for that ring. The Cisco TFTP server for each Cisco Unified Communications Manager contains this file.

The `CiscoIPconference stationRingList` XML object uses the following simple tag set to describe the information:

```
<CiscoIPconference stationRingList>
 <Ring>
 <DisplayName/>
 <FileName/>
 </Ring>
</CiscoIPconference stationRingList>
```

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

- `DisplayName` defines the name of the custom ring for the associated PCM file that will display on the Ring Type menu of the conference 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.

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

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

# PCM File Requirements for Custom Ring Types

The PCM files for the ring types must meet the following requirements for proper playback on conference phones:

- Raw PCM (no header)
- 16000 samples per second
- 16 bits per sample
- Least Significant Bit
- Minimum ring size is 240 samples
- Number of samples in the ring is evenly divisible by 240
- Maximum ring duration is 10 seconds
- Ring starts and ends at the zero crossing
- To create PCM files for custom conference phone rings, you can use any standard audio editing packages that support these file format requirements

# Set Up Custom Ringtone

To create custom conference phone rings for the conference phone, follow 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 the PCM File Requirements for Custom Ring Types, on page 103 section.

**Step 2** Upload the new PCM files that you created to the Cisco TFTP server for each Cisco Unified Communications Manager in your cluster. For more information, see the *Cisco Unified Communications Operating System Administration Guide*, “Software Upgrades” chapter.

**Step 3** Use a text editor to edit the `Ringlist-wb.xml` file. See the Ringlist-wb.xml File Format Requirements, on page 102 section for information about how to format this file and for a sample `Ringlist-wb.xml` file.

**Step 4** Save your modifications and close the `Ringlist-wb.xml` file.

**Step 5** Cache the new `Ringlist-wb.xml` file:

a) Log on to Cisco Unified Communications Manager Administration.
b) From the Navigation drop-down list at the top right of the window, select **Cisco Unified Serviceability**, and then press **Go**.
c) Choose **Tools** > **Control Center - Feature Services**.

d) In the CM Services area, locate, stop, and start the Cisco TFTP service.

# Idle Display Setup

You can specify an idle display that appears on the conference phone LCD screen. The idle display is an XML service that the conference phone invokes when the conference phone has been idle (not in use) for a designated period and no feature menu is open.

XML services that can be used as idle displays include company logos, product pictures, and stock quotes.

Configuring the idle display consists of these general steps:

1. Formatting an image for display on the conference phone.
2. Configuring Cisco Unified Communications Manager to display the image on the conference phone.

For detailed instructions about creating and displaying the idle display, see *Creating Idle URL Using Graphics on Cisco IP Phone* at this URL:
http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_tech_note09186a00801c0764.shtml.

In addition, you can see the *Cisco Unified Communications Manager Administration Guide* or to *Cisco Unified Communications Manager Bulk Administration Guide* for the following information:

- Specifying the URL of the idle display XML service:
  - For a single conference phone: Idle field on the Phone Template Configuration page in the Bulk Administration Tool (BAT)
  - For multiple conference phones simultaneously: URL Idle Time field on the Cisco Unified Communications Manager Enterprise Parameters page, or the Idle field in the Bulk Administration Tool (BAT)
- Specifying the length of time that the conference phone is not used before the idle display XML service is invoked:
  - For a single conference phone: Idle Timer field on the Cisco Unified Communications Manager Administration Phone Configuration page
  - For multiple conference phones simultaneously: URL Idle Time field on the Cisco Unified Communications Manager Administration Enterprise Parameters Configuration page, or the Idle Timer field in the Bulk Administration Tool (BAT)

From a conference phone, you can see settings for the idle display XML service URL and the length of time that the conference phone is not used before this service is invoked. To see these settings, choose **Apps** > **Settings** > **Device Configuration** > **HTTP Configuration**, and then scroll to the Idle URL and the Idle URL Time parameters.

CHAPTER 10

# Model Information, Status, and Statistics

## Model Information, Status, and Statistics Overview

This chapter describes how to use the following menus and screens on the Cisco Unified IP Conference Phone to view conference station information such as model, device, and network information:

- Model Information screen: Displays hardware and software information about the conference phone.
- Status menu: Provides access to screens that display network and call statistics and device information.

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

You can also obtain much of this information, and obtain other related information, remotely through the conference phone web page. For more information, see Remote Monitoring, on page 111.

For more information about troubleshooting the conference phone, see Troubleshooting and Maintenance, on page 121.

**Note** There are certain options on the Network Configuration menu, Device Configuration menu, and Security Configuration menu that are for display only. These options are described in Cisco Unified IP Conference Phone Settings, on page 59.

## Model Information Screen

The Model Information screen displays this information:

- Model Number: Model number of the conference phone.
- MAC Address: Media Access Control (MAC) address of the conference phone.
- Software Version: Version of the firmware running on the conference phone.

- BootROM Version: Identifier of the factory-installed load running on the conference phone.
- App Load ID: Identifies the firmware running on the conference phone.
- Active load:xxx: Current active firmware running on the conference phone.
- Inactive load: xxx: Inactive firmware kept on the conference phone.
- Last Upgrade: <time date>: Time and date for last firmware upgrade
- Active Server: xxx: Current active server.
- Stand-by-Server:xxx: Current stand by server.
- Mic 1: (xx) connected/disconnected: Mic connection state
- Mic 2: (xx) connected/disconnected: Mic connection state
- Wireless Mic 1ID: Mic ID
- Wireless Mic 2ID: Mic ID
- System ID:xxx: System ID
- Linked Mode: ON/OFF: Linked mode state
- Backlight On Time: <time>: Back light on time
- Backlight On Duration: <time>: Back light on duration
- Days Backlight Not Active: <days>: Days of the week when backlight is inactive

## Display Model Information Screen

### Procedure

**Step 1** To display the Model Information screen, press the **Settings** button and then select **Model Information**.

**Step 2** To exit the Model Information screen, press **Exit**.

# Status Menu

The Status menu includes these options, which provides information about the conference phone and its operation:

- Network Statistics: Displays the Network Statistics screen, which shows Ethernet traffic statistics.
- Call Statistics: Displays information about the last call on the conference phone.
- Device Information: Displays device settings and related information for the conference phone.

**Note** The Status menu also contains a Ping menu that allows you to test network connectivity to another conference phone.

## Display Status Menu

### Procedure

**Step 1** Press **Apps**.

**Step 2** Select **Admin Settings** > **Status Menu**.

## Network Statistics Screen

The Network Statistics screen displays information about the conference phone and network performance.

The following table describes the information that appears in this screen.

*Table 32: Network Statistics Items*

| Item | Description |
|---|---|
| Rx Frames | Number of packets received by the conference phone. |
| Rx Broadcasts | Number of broadcast packets received by the conference phone. |
| Rx Unicast | Total number of unicast packets received by the conference phone. |
| Tx Frames | Number of packets transmitted by the conference phone. |
| Tx Broadcasts | |
| Tx Unicast | |
| CDP Neighbor Device ID | |
| CDP Neighbor IP Address | |
| CDP Neighbor Port | |
| Restart Cause | Displays the cause of a restart, for example: `Port X 100 Full`. |
| IPv4 | Displays the message: `DHCP DISABLED` or `DHCP ENABLED`. |

## Display Network Statistics Screen

To display the Network Statistics screen, perform these steps:

**Procedure**

**Step 1** Press **Applications**.

**Step 2** Select **Settings**.

**Step 3** Select **Status**.

**Step 4** Select **Network Statistics**.

**Step 5** To reset the Rx Frames, Tx Frames, and Rx Broadcasts statistics to 0, press **Clear**.

# Call Statistics Screen

The Call Statistics screen displays information about the last call on the conference phone.

**Note** You can remotely view the call statistics information by using a web browser to access the Streaming Statistics web page. For more information about remote monitoring, see Remote Monitoring, on page 111.

A single call can have multiple voice streams, but data is captured for only the last voice stream. A voice stream is a packet stream between two endpoints. If one endpoint is put on hold, the voice stream stops even though the call is still connected. When the call resumes, a new voice packet stream begins, and the new call data overwrites the former call data.

## Call Statistics Information

The following table describes the information displayed on the screen.

*Table 33: Call Statistics Items*

| Item | Description |
|---|---|
| Receiver Codec Type (Rcvr Codec) | Type of voice stream received (RTP streaming audio): G.729, G.711 u-law, G.711 A-law, G.722, G.722.1, or Lin16k. |
| Sender Codec Type | Type of voice stream transmitted (RTP streaming audio): G.729, G.711 u-law, G.711 A-law, G.722, or Lin16k. |
| Receiver Size (Rcvr Size) | Number of bytes of voice packets received since voice stream was opened. |
| Sender Size | Number of bytes of voice packets sent since voice stream was opened. |

| Item | Description |
|---|---|
| Rcvr Packets | Number of RTP voice packets received since voice stream was opened.<br>**Note** This number is not necessarily identical to the number of RTP voice packets received since the call began because the call might have been placed on hold. |
| Sender Packets | Number of RTP voice packets transmitted since voice stream was opened.<br>**Note** This number is not necessarily identical to the number of RTP voice packets transmitted since the call began because the call might have been placed on hold. |
| Avg Jitter | Estimated average RTP packet jitter (dynamic delay that a packet encounters when going through the network) observed since the receiving voice stream was opened. |
| Max Jitter | Maximum jitter observed since the receiving voice stream was opened. |
| Rcvr Discarded | Number of RTP packets discarded by the receiver. |
| 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 8-second interval of the voice stream. |
| Avg MOS LQK | Average MOS LQK score observed for the entire voice stream. |
| Min MOS LQK | Lowest MOS LQK score observed from start of the voice stream. |
| Max MOS LQK | Baseline or highest MOS LQK score observed from start of the voice stream. |
| Cumulative Conceal Ratio | Total number of concealment frames divided by total number of speech frames received from start of the voice stream. |
| Max Conceal Ratio | Maximum concealment ratio that is observed during the call. |
| Conceal Secs | Number of seconds that have concealment events (lost frames) from the start of the voice stream (includes severely concealed seconds). |

| Item | Description |
|---|---|
| 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 Call Statistics Screen

To display the Call Statistics screen for information about the last voice stream, follow these steps:

### Procedure

**Step 1** Press **Settings**.

**Step 2** Select **Status**.

**Step 3** Select **Call Statistics**.

CHAPTER 11

# Remote Monitoring

## Remote Monitoring Overview

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

- Device information
- Network configuration information
- Ethernet information
- Device logs
- Streaming statistics

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

You can also obtain much of this information directly from a conference phone. For more information, see Model Information, Status, and Statistics, on page 105.

For more information about troubleshooting the conference phone, see Troubleshooting and Maintenance, on page 121.

# Access Web Page

**Note** If you cannot access the web page, it may be disabled. See the Control Web Page Access, on page 113 section for more information.

### Procedure

**Step 1** Obtain the IP address of the conference phone using one of these methods:

- From Cisco Unified Communications Manager Administration, choose **Device** > **Phone**. Enter search criteria to locate the conference phone, and then click the conference phone name. Conference phones registered with Cisco Unified Communications Manager display the IP address at the top of the Phone Configuration web page.
- On the conference phone, choose **Apps** > **Settings** > **Network Configuration**. 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 conference phone: http://<*IP_address*>

# Web Page Information

The web page for a conference phone includes these hyperlinks:

- **Device Information**: Displays device settings and related information for the conference phone.
- **Network Configuration**: Displays network configuration information and information about other conference phone settings.
- **Ethernet Information**: Displays network statistics.
- **Device Logging**: Displays messages that might be useful to Cisco TAC if you require assistance with troubleshooting.
- **Streaming Statistics**: Displays call statistics.

### Related Topics

Device Information Area, on page 113
Network Configuration Area, on page 114
Ethernet Information Area, on page 117
Device Logs Area, on page 118
Streaming Statistics Area, on page 118

# Control Web Page Access

For security purposes, you may choose to prevent access to the web pages for a conference phone. If you do so, you will prevent access to the web pages that are described in this chapter and to the Cisco Unified Communications Manager Self Care Portal.

To enable or disable access to the web pages for a conference phone, follow these steps from Cisco Unified Communications Manager Administration:

### Procedure

**Step 1** Choose **Device** > **Phone**.

**Step 2** Specify the criteria to find the phone and click **Find**, or click **Find** to display a list of all phones.

**Step 3** Click the device name to open the Phone Configuration web page for the device.

**Step 4** In the Product Specific Configuration Layout area, from the Web Access drop-down list, choose **Enabled or Disabled**.

**Step 5** Click **Update**.

**Note** Some features, such as Cisco Quality Report Tool, do not function properly without access to the conference phone web pages. Disabling web access also affects any serviceability application that relies on web access, such as CiscoWorks.

# Device Information Area

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

To display the Device Information area, access the web page for the conference phone as described in the Access Web Page, on page 112 section, and then click the **Device Information** hyperlink.

*Table 34: Device Information Area Items*

| **Item** | |
|---|---|
| MAC Address | Media Access Control (MAC) address of the conference phone. |
| Host Name | Unique, fixed name that is automatically assigned to the conference phone based on its MAC address. |
| DN | Directory number assigned to the conference phone. |
| Version | Version of the firmware running on the conference phone. |
| Hardware Revision | Revision value of the conference phone hardware. |
| Serial Number | Serial number of the conference phone. |

| Item | |
|---|---|
| Model Number | Model number of the conference phone. |
| Message Waiting | Indicates if there is a voice message waiting for this conference phone. |
| UDI | Displays the following Cisco Unique Device Identifier (UDI) information about the conference phone:<br>• Device Type: Indicates hardware type. For example, *phone* displays for all phone models<br>• Device Description: Displays the name of the conference phone associated with the indicated model type<br>• Product Identifier: Specifies the conference phone model<br>• Serial Number: Displays the conference phone unique serial number |
| Time | Time obtained from the Date/Time Group in Cisco Unified Communications Manager to which the conference phone belongs. |
| Time Zone | Time zone obtained from the Date/Time Group in Cisco Unified Communications Manager to which the conference phone belongs. |
| Date | Date obtained from the Date/Time Group in Cisco Unified Communications Manager to which the conference phone belongs. |

# Network Configuration Area

The Network Configuration area on a conference phone web page displays network configuration information and information about other conference phone settings. The following table describes this information.

You can view and set many of these items from the Network Configuration Menu and the Device Configuration Menu on the conference phone.

To display the Network Configuration area, access the web page for the conference phone as described in the Access Web Page, on page 112 section, and then click the **Network Configuration** hyperlink.

| Item | Description |
|---|---|
| DHCP Enabled | Indicates whether DHCP is being used by the conference phone. |
| MAC Address | MAC address of the conference phone. |
| Host Name | Host name that the DHCP server assigned to the conference phone. |
| IP Address | IP address of the conference phone. |
| Subnet Mask | IP address of the subnet mask used by the conference phone. |
| Default Router 1 | Default router used by the conference phone (Default Router 1). |

| Item | Description |
|---|---|
| Domain Name | Name of the Domain Name System (DNS) domain in which the conference phone resides. |
| DNS Server 1–5 | Primary Domain Name System (DNS) server (DNS Server 1) and optional backup DNS servers (DNS Server 2–5) used by the conference phone. |
| Operational VLAN ID | Auxiliary Virtual Local Area Network (VLAN) configured on a Cisco Catalyst switch in which the conference phone is a member. |
| Admin. VLAN ID | Auxiliary VLAN in which the conference phone is a member. |
| TFTP Server 1 | Primary Trivial File Transfer Protocol (TFTP) server used by the conference phone. |
| TFTP Server 2 | Optional backup TFTP server that the conference phone uses if the primary TFTP server is unavailable. |
| Alternate TFTP | Indicates whether the conference phone is using an alternate TFTP server. |
| Ethernet Configuration | Speed and duplex of the Ethernet port (labeled LAN on the conference phone). |
| CallManager 1–5 | Host names or IP addresses, in prioritized order, of the Cisco Unified Communications Manager servers with which the conference phone can register. An item can also show the IP address of a Survivable Remote Site Telephony (SRST) router that is capable of providing limited Cisco Unified Communications Manager functionality, if such a router is available.<br>For an available server, an item will show the Cisco Unified Communications Manager server IP address and one of the following states:<br>• Active: Cisco Unified Communications Manager server from which the conference phone is currently receiving call-processing services.<br>• Standby: Cisco Unified Communications Manager server to which the conference phone switches if the current server becomes unavailable.<br>• Blank: No current connection to this Cisco Unified Communications Manager.<br>An option may also include the SRST designation, which indicates 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. |
| Information URL | URL of the help text that appears on the conference phone. |

| Item | Description |
|---|---|
| Services URL | URL of the server from which the conference phone obtains conference phone services. |
| Directories URL | URL of the server from which the conference phone obtains directory information. |
| Messages URL | URL of the server from which the conference phone obtains message services. |
| Authentication URL | URL that the conference phone uses to validate requests made to the conference phone web server. |
| Proxy Server URL | URL of proxy server, which makes HTTP requests to non-local host addresses on behalf of the conference phone HTTP client and provides responses from the non-local host to the conference phone HTTP client. |
| Idle URL | URL that the conference phone displays when the conference phone has not been used for the time specified by Idle URL Time and no menu is open. |
| Idle URL Time | Number of seconds that the conference phone has not been used and no menu is open before the XML service specified by Idle URL is activated. |
| User Locale | User locale associated with the conference phone user. Identifies a set of detailed information to support users, including language, font, date and time formatting, and alphanumeric keyboard text information. |
| User Locale Version | Version of the user locale loaded on the conference phone. |
| User Locale Char Set | Version of the character set that the conference phone uses for the user locale. |
| Network Locale | Network locale associated with the conference phone user. Identifies a set of detailed information to support the conference phone in a specific location, including definitions of the tones and cadences used by the conference phone. |
| Network Locale Version | Version of the network locale loaded on the conference phone. |
| DSCP For Call Control | DSCP IP classification for call control signaling. |
| DSCP For Configuration | DSCP IP classification for any conference phone configuration transfer. |
| DSCP For Services | DSCP IP classification for conference phone-based services. |
| Web Access Enabled | Indicates whether web access is enabled (Yes) or disabled (No) for the conference phone. |

### Related Topics

Cisco Unified IP Conference Phone Settings, on page 59

# Ethernet Information Area

The Ethernet Information area on a conference phone web page provides information about network traffic on the conference phone, such as:

- Ethernet traffic
- Network traffic to and from the PC port on the conference phone
- Network traffic to and from the network port on the conference phone

To display the Ethernet Information area, access the web page for the conference phone as described in the Access Web Page, on page 112 section, and then click the **Ethernet Information** hyperlink.

The following table describes the information in the Ethernet Information area.

*Table 35: Ethernet Information Area Items*

| Item | Description |
|---|---|
| Rx error | Total number of FCS error packets or Align error packets received. |
| Rx PacketNoDes | Total number of shed packets caused by no DMA descriptor. |
| Rx Overruns | Total number of received packets dropped because of buffer overruns. |
| Rx alignErr | Total number of packets received between 64 and 1522 bytes in length that have bad FCS errors. |
| Rx length error | Number of packets discarded due to improper length. |
| Rx symbol error | Number of valid length packets received that have at least one invalid data symbol. |
| Rx CRC Errors | Total number of packets received with CRC failed. |
| Rx Broadcasts | Number of broadcast packets received by the conference phone. |
| Rx Multicasts | Total number of multicast packets received by the conference phone. |
| Rx fail filter | Total number of packets received by the conference phone that failed. |
| Rx VLAN | Total number of packets received on the Virtual Local Area Network. |
| Rx control frames | Total number of control frames received. |
| Rx unicast | Total number of unicast packets received by the conference phone. |
| Tx error | Total number of FCS error packets or Align error packets transmitted by the conference phone. |
| Tx no descriptor | Total number of transmit packets dropped because no descriptor was specified. |
| Tx fifoUnderrun | Total number of transmit packets dropped because of fifo underrun. |

| Item | Description |
|---|---|
| Tx lateCollision | Number of times that collisions occurred later than 512 bit times after the start of packet transmission. |
| Tx Excessive Collisions | Total number of packets that could not be sent because of network congestion. |
| Tx excessDefer | Total number of packets delayed from transmitting due to medium being busy. |
| Tx Deferred Abort | Total number of transmit packets aborted. |
| Tx Collisions | Total number of collisions that occurred while a packet was being transmitted. |
| Event send failed | Total number of packets that failed to transmit. |
| Event Rx packet send failed | Total number of packets that were not received. |
| Tx excessLength | Total number of packets not transmitted because the packet experienced 16 transmission attempts. |
| Rx totalPkt | Total number of packets received by the conference phone. |
| Packet Transmitted | Total number of packets transmitted by the conference phone. |
| Rcvr Octets | Total number of octets received by the conference phone. |
| Sender Octets | Total number of octets sent by the conference phone. |

# Device Logs Area

The Device Logs area on a conference phone web page provides information you can use to help monitor and troubleshoot the conference phone. It includes debug and error messages received on the conference phone that might be useful to Cisco TAC if you require assistance with troubleshooting.

To display device logs, access the web page for the conference phone as described in the Access Web Page section, and then click the **Device Logging** hyperlink. In the File Download dialog box, click **Open** to view the device logs, or click **Save** to save the logs to a specific location.

# Streaming Statistics Area

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

The Streaming Statistics area on a conference phone web page provides information about the streams. Most calls use only one stream (Stream 1), but some calls use two or three streams. For example, a barged call uses Stream 1 and Stream 2.

To display the Streaming Statistics area, access the web page for the conference phone as described in the Access Web Page, on page 112 section, and then click the **Streaming Statistics** hyperlink.

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

*Table 36: Streaming Statistics Area Items*

| Item | Description |
|---|---|
| Remote Address | IP address and UDP port of the stream. |
| Local Address | IP address and UDP port of the conference phone. |
| Start Time | Internal time stamp indicating when Cisco Unified Communications Manager requested that the conference phone start transmitting packets. |
| Codec Type | Type of voice stream received or transmitted (RTP streaming audio): G.729, G.711 u-law, G.711 A-law, G.722, or Lin16k. |
| Payload Size | Size of voice packets, in milliseconds, in the receiving or transmitting voice stream (RTP streaming audio). |
| Rcvr Packets | Number of RTP voice packets received since voice stream was opened.<br>**Note** This number is not necessarily identical to the number of RTP voice packets received since the call began because the call might have been placed on hold. |
| Rcvr Lost Packets | Missing RTP packets (lost in transit). |
| Rcvr Octets | Number of bytes of voice packets received since voice stream was opened. |
| Rx Expected Pkts | The expected number of packets received for the local conference phone. |
| Last Rx Seq No | The sequence number of the last RTP packet received. |
| Most recent Rx SSRC | The Synchronization Source field of the last RTP packet received. |
| Avg Jitter | Estimated average RTP packet jitter (dynamic delay that a packet encounters when going through the network) observed since the receiving voice stream was opened. |
| Max Jitter | Maximum jitter observed since the receiving voice stream was opened. |
| Sender Packets | Number of RTP voice packets transmitted since voice stream was opened.<br>**Note** This number is not necessarily identical to the number of RTP voice packets transmitted since the call began because the call might have been placed on hold. |
| Sender Octets | Number of bytes of voice packets transmitted since voice stream was opened. |

CHAPTER 12

# Troubleshooting and Maintenance

# Call, Device, and Network Information

You can view call, device, and network information through the Applications menu, or remotely through each conference phone web page. You can use this information to monitor the operation of a conference phone to assist with troubleshooting.

**Related Topics**

Model Information, Status, and Statistics, on page 105

Remote Monitoring, on page 111

# Troubleshooting

Use the following sections to troubleshoot problems with the conference phone.

## Startup Problems

After installing a conference phone into your network and adding it to Cisco Unified Communications Manager, the conference phone should start up as described in IP Phone Startup Verification, on page 53. If the conference phone does not start up properly, see the following sections for troubleshooting information.

### Cisco Unified IP Phone Does Not Go Through the Normal Startup Process

**Problem**

When you connect a conference phone into the network port, the conference phone should go through its normal startup process, and the LCD screen should display information.

#### Cause

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

#### Solution

To determine whether the conference phone is functional, follow these suggestions to systematically eliminate these other potential problems:

- Verify that the network port is functional:
  - Exchange the Ethernet cables with cables that you know are functional.
  - Disconnect a functioning conference phone from another port and connect it to this network port to verify the port is active.
  - Connect the conference phone that will not start up to a different network port that is known to be good.
  - Connect the conference phone that will not start up directly to the port on the switch, eliminating the patch panel connection in the office.
- Verify that the conference 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 conference phone still does not start up properly, perform a factory reset of the conference phone.

If after attempting these solutions, the LCD screen on the conference phone does not display any characters after at least five minutes, contact a Cisco technical support representative for additional assistance.

#### Related Topics

IP Phone Startup Verification, on page 53
Cisco Unified IP Conference Phone Reset or Restore, on page 134
Conference Phone Power, on page 35

## Cisco Unified IP Phone Does Not Register with Cisco Unified Communications Manager

To start up properly, the conference phone must be connected to the Ethernet network and registered with a Cisco Unified Communications Manager. If the conference phone does not start up properly, review the following sections.

### TFTP Server Settings

#### Problem

The TFTP server settings may not be correct.

#### Solution

Check the TFTP settings. See Check TFTP Settings, on page 131.

### IP Addressing and Routing

#### Problem

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

#### Solution

You should verify the Internet Protocol (IP) addressing and routing settings on the conference phone. If you are using DHCP, the DHCP server should provide these values. If you have assigned a static IP address to the conference phone, you must enter these values manually. See Check DHCP Settings, on page 133

### DNS Settings

#### Problem

The DNS settings may be incorrect.

#### Solution

If you are using DNS to see the TFTP server or to Cisco Unified Communications Manager, you must ensure that you have specified a Domain Name System (DNS) server. See Verify DNS Settings, on page 133

## Cisco Unified Communications Manager and TFTP Servers Are Not Running

If the Cisco Unified Communications Manager or TFTP services are not running, conference phones may not be able to start up properly. However, in such a situation, it is likely that you are experiencing a system-wide failure and that other conference phones and devices are unable to start up properly.

If the Cisco Unified Communications Manager service is not running, all devices on the network that rely on it to make conference phone calls will be affected. If the TFTP service is not running, many devices will not be able to start up successfully For more information, see Start Service, on page 132.

## Configuration File Corruption

#### Problem

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

#### Solution

Create a new configuration file. See Create New Phone Configuration File, on page 133.

## Cisco Unified Communications Manager Phone Registration

#### Problem

The conference phone is not registered with the Cisco Unified Communications Manager.

### Solution

A conference phone can register with a Cisco Unified Communications Manager server only if the conference phone has been added to the server or if autoregistration is enabled. Review the information and procedures in the Cisco Unified Communications Manager Administration Conference Station Addition, on page 41 section to ensure that the conference phone has been added to Cisco Unified Communications Manager.

To verify that the conference phone is in the Cisco Unified Communications Manager database, choose **Device** > **Phone** from Cisco Unified Communications Manager Administration and search for the conference phone based on its MAC Address. For information about determining a MAC address, see the Conference Phone MAC Address Determination, on page 42 section.

If the conference phone is already in the Cisco Unified Communications Manager database, its configuration file may be damaged. See the Configuration File Corruption, on page 123 section for assistance.

# Cisco Unified IP Conference 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 conference phone is connected 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 Conference Phone Resets Unexpectedly

If users report that their phones are resetting during calls or while idle on their desk, you should investigate the cause. If the network connection and Cisco Unified Communications Manager connection are stable, a phone should not reset on its own.

Typically, a phone resets if it has problems connecting to the Ethernet network or to Cisco Unified Communications Manager. The following sections can help you identify the cause of a conference phone resetting in your network.

## Physical Connection Problems

### Problem

The physical connection to the LAN may be broken.

### Solution

Verify that the Ethernet connection to which the phone is connected is up. For example, check if the particular port or switch to which the phone is connected is down and that the switch is not rebooting. Also make sure that there are no cable breaks.

## Intermittent Network Outages

### Problem

The conference phone resets because the 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 network administrator for information on known problems in the voice network.

## DHCP Setting Errors

### Problem

The DHCP settings may be incorrect.

### Solution

Follow this process to help determine if the phone has been properly configured to use DHCP:

1. Verify that you have properly configured the conference phone to use DHCP. See the Network Setup Menu, on page 62 section for more information.
2. Verify that the DHCP server has been set up properly.
3. Verify the DHCP lease duration. Cisco recommends that you set it to 8 days.

   conference phones send messages with request type 151 to renew their DHCP address leases. If the DHCP server expects messages with request type 150, the lease will be denied, forcing the conference phone to restart and request a new IP address from the DHCP server.

## Static IP Address Setting Errors

### Problem

The status IP address assigned to the conference phone may be incorrect.

### Solution

If the conference phone has been assigned a static IP address, verify that you have entered the correct settings. See the Network Setup Menu, on page 62 section more information.

## Voice VLAN Setup Errors

### Problem

If the conference phone appears to reset during heavy network usage (for example, following extensive web surfing on a computer connected to the same switch as conference phone), it is likely that you do not have a voice VLAN configured.

### Solution

Isolating the conference phones on a separate auxiliary VLAN increases the quality of the voice traffic. See the Cisco Unified IP Communications Product Interactions, on page 33 section for details.

## DNS or Other Connectivity Errors

### Problem

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

### Solution

If the conference phone continues to reset, follow the procedure in Determine DNS or Connectivity Issues, on page 132.

# Power Connection Problems

### Problem

The conference station does not appear to be powered up.

### Solution

In most cases, a conference phone will restart if it powers up using external power but loses that connection and switches to Power over Ethernet (PoE). Similarly, a conference phone may restart if it powers up using PoE and then gets connected to an external power supply.

# Audio and Display Problems

The following sections describe how to resolve audio and display problems.

## Display Is Wavy

### Problem

The display appears to have rolling lines of a wavy pattern.

### Cause

The conference phone might be interacting with certain types of older fluorescent lights in the building.

### Solution

Move the conference phone away from the lights or replace the lights to resolve the problem.

## Choppy Speech or Sound

### Problem

A user complains of choppy speech or a metallic sound coming from or going to the far end.

### Cause

There may be jitter in the network or too many dropped packets.

### 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. For more information about displaying statistics, see Call Statistics Screen, on page 108.

## Choppy Speech or Sound When Using Wireless Microphones

### Problem

A user complains of choppy speech or metallic sound coming from the wireless microphones.

### Cause

Too many dropped packets.

### Solution

Check the RF environment

## Echo on Far End

### Problem

The far end hears echo.

### Cause

You may be experiencing one of the following:

- The conference phone is not on a flat and stable surface.
- The wired or wireless microphones are too close to the sound base.
- The wired or wireless microphones are not on a flat and stable surface.
- In Linked Mode, the primary and secondary sound base units are too close together.

### Solution

Check the placement of the bases and microphones.

## Audio Level Too Low

### Problem

A user complains that the audio level is too low.

### Cause

You may be experiencing one of the following:

- The user is not facing the conference phone when speaking.
- The user is too far from the conference phone when speaking.
- The wireless microphones are being moved.

### Solution

Consider using external microphones, or increasing the room coverage by using Linked Mode.

## Audio Quality Poor

### Problem

User complains about poor audio quality.

### Cause

You are using a narrow band rather than a wide band codec.

### Solution

Verify on the CUCM that the default codec is G.722 (wide band).

## No Audio Between Units

### Problem

There is no audio to or from the secondary unit in Linked Mode.

### Cause

The daisy cable is not connected properly.

### Solution

- Verify that the daisy cable is properly seated and that it is routed inside the cable grooves.
- Verify that the external microphone icon is present on the display if one is connected.

## No Audio from External Wireless Microphones

### Problem

There is no audio to or from the external wireless microphones.

### Cause

The wireless microphones are not paired or are not linked with the device.

### Solution

- Verify that the wireless microphone is paired and that the wireless microphone icon is present on the display.
- Verify that the LED on the wireless external microphone is flashing green.
- Verify that the wireless microphone is charged.

## Conference Call Reception Problems

To ensure optimum performance with the conference phone and the external microphones, see Performance Guidelines, on page 51.

## General Troubleshooting Information

This section provides troubleshooting information for some common issues that might occur on the conference phone.

The following table provides general troubleshooting information for the conference phone.

*Table 37: Cisco Unified IP Conference Phone Troubleshooting*

| Summary | Explanation |
|---|---|
| Changing the conference phone 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. |
| Codec mismatch between the conference phone and another device | The RxType and the TxType statistics show the codec that is being used for a conversation between this conference 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.<br>See Call Statistics Screen, on page 108 for information about displaying these statistics. |
| Dual-Tone Multi-Frequency (DTMF) delay | When you are on a call that requires keypad input, if you press the keys too quickly, some of them might not be recognized. |
| conference phone does not ring | Check that the ringer setting is not “Ringer Off.” Check the volume level. |

| Summary | Explanation |
|---|---|
| Loopback condition | A loopback condition can occur when the following conditions are met:<br>• The conference phone receives power from an external power supply<br>• The conference phone is powered down (the power supply is disconnected)<br>In this case, the switch port on the conference phone can become disabled and the following message will appear in the switch console log:<br>`HALF_DUX_COLLISION_EXCEED_THRESHOLD`<br>To resolve this problem, re-enable the port from the switch. |
| Moving a network connection from the conference phone to a workstation | If you are powering your conference phone through the network connection, you must be careful if you decide to unplug the conference phone network connection and plug the cable into a desktop computer.<br>**Caution** The computer’s network card 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 conference phone before plugging it into a computer. This delay gives the switch enough time to recognize that there is no longer a conference phone on the line and to stop providing power to the cable. |
| No dial tone | Check that all connections are secure and in place. Make sure all connections are correct. |
| No LCD screen display | Check to make sure that the conference phone has power. Make sure that the power supply unit is plugged in. |
| One-way audio | When at least one person in a call does not receive audio, IP connectivity between conference phones is not established. Check the configurations in routers and switches to ensure that IP connectivity is properly configures. |

| Summary | Explanation |
|---|---|
| Poor voice quality when calling digital cell conference phones using the G.729 codec (protocol)<br>**Caution** Using a cell, mobile, or GSM conference phone, or two-way radio in close proximity to a Cisco Unified IP Conference Phone 8831 might cause interference. For more information, see the manufacturer's documentation of the interfering device. | In Cisco Unified Communications Manager, you can configure the network to use the G.729 protocol (the default is G.711). When using G.729, calls between a Cisco Unified IP Conference Phone and a digital cellular conference phone will have poor voice quality. Use G.729 only when absolutely necessary.<br>For more information, see the Cisco Unified Communications Manager application online help. |
| Prolonged broadcast storms cause conference 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 conference phones to reset, lose an active call, or be unable to initiate or answer a call. conference phones may not come up until a broadcast storm ends. |
| Sound sample mismatch between the conference phone and another device | The RxSize and the TxSize statistics show the size of the voice packets that are being used in a conversation between this conference phone and the other device. The values of these statistics should match.<br>See Call Statistics Screen, on page 108 for information about displaying these statistics. |

# 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 used by the conference phone by choosing **Apps** > **Admin Settings** > **Network Setup** > **IPv4 Configuration** > **TFTP Server 1** .

**Step 2** If you have assigned a static IP address to the conference phone, you must manually enter a setting for the TFTP Server 1 option.

**Step 3** If you are using Dynamic Host Configuration Protocol (DHCP), the conference phone obtains the address for the Trivial File Transfer Protocol (TFTP) server from the DHCP server. A valid TFTP server must be set in DHCP option 150 or option 66 on the DHCP server.

**Step 4** You can also enable the conference phone to use an alternate TFTP server. Such a setting is particularly useful if the conference phone was recently moved from one location to another.

### Related Topics

Network Setup Menu, on page 62

## Start Service

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 that displays in the upper, right corner of the window, and then click **Go**.

**Step 2** Choose **Tools** > **Control Center - Network Services**.

**Step 3** Choose the primary Cisco Unified Communications Manager server from the Server drop-down list.

The page displays the service names for the server that you chose, the status of the services, and a service control panel to stop or start a service.

**Step 4** If a service has stopped, click its radio button, and then click **Start**.

## Determine DNS or Connectivity Issues

Use these steps to eliminate DNS or other connectivity errors:

### Procedure

**Step 1** Navigate to **Apps** > **Admin Settings** > **Network Setup** > **IPv4 Configuration** > **DHCP** and choose the Reset All option to reset conference phone settings to their default values.

**Step 2** Modify DHCP and IP settings:

a) Disable DHCP.

b) Assign static IP values to the conference phone. Use the same default router setting used for other functioning conference phones.

c) Assign TFTP server. Use the same TFTP server used for other functioning conference phones.

**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 Administration, choose **System > Server** to locate the server, and then click the server name. Verify that the server is referred to by its IP address and not by its DNS name.

**Step 5** From Cisco Unified Communications Manager Administration, choose **Device > Phone** to locate the conference phone, and then click the conference phone name. Verify that you have assigned the correct MAC address to this conference phone.

**Step 6** Power cycle the conference phone.

### Related Topics

Cisco Unified IP Conference Phone Reset or Restore, on page 134

Network Setup Menu, on page 62

Conference Phone MAC Address Determination, on page 42

## Create New Phone Configuration File

**Note** When you remove a conference phone from the Cisco Unified Communications Manager database, its configuration file is deleted from the Cisco Unified Communications Manager TFTP server. The conference phone directory number remains in the Cisco Unified Communications Manager. It becomes an “unassigned DN” and can be used by another device. If unassigned DNs are not used by other devices, delete them from Cisco Unified Communications Manager. You can use the Route Plan Report to view and delete unassigned reference numbers. For more information, see *Cisco Unified Communications Manager Administration Guide*.

To create a new configuration file, follow these steps:

### Procedure

**Step 1** In Cisco Unified Communications Manager Administration, choose **Device** > **Phone**. Enter search criteria to locate the conference phone experiencing problems, and then click the device name.

**Step 2** In the Phone Configuration window, click **Delete** to remove the conference phone from Cisco Unified Communications Manager.

**Step 3** Add the conference phone to Cisco Unified Communications Manager.

**Step 4** Power cycle the conference phone.

### Related Topics

Cisco Unified Communications Manager IP Phone Addition Methods, on page 39

## Verify DNS Settings

To verify DNS settings, follow these steps:

### Procedure

**Step 1** Select **Apps** > **Admin Settings** > **Network Setup** > **IPv4 Configuration** > **DNS Server 1**.

**Step 2** Verify that there is a CNAME entry in the DNS server for the TFTP server and one for Cisco Unified Communications Manager.

**Step 3** Ensure that DNS is configured to do reverse look-ups.

## Check DHCP Settings

**Note** DHCP can be enabled and disabled manually.

**Procedure**

**Step 1** On the conference station, select **Apps** > **Admin Settings** > **Network Setup** > **IPv4 Configuration**, and look at the following options:

- DHCP: If you have assigned a static IP address to the conference 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 it does not, check your IP routing and VLAN configuration. See *Troubleshooting Switch Port Problems*, 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 conference phone, you must manually enter settings for these options.

**Step 2** If you are using DHCP, check the IP addresses distributed by your DHCP server. See *Understanding and Troubleshooting DHCP in Catalyst Switch or Enterprise Networks*, available at this URL: http://www.cisco.com/c/en/us/support/docs/ip/dynamic-address-allocation-resolution/27470-100.html

**Related Topics**

Network Setup Menu, on page 62

## Additional Troubleshooting Information

If you have additional questions about troubleshooting the conference phone, several Cisco.com web sites can provide you with more tips. Choose from the sites available for your access level.

- Conference Phone Troubleshooting Resources: http://www.cisco.com/en/US/products/hw/phones/ps379/tsd_products_support_series_home.html
- Cisco Products and Services (Technical Support and Documentation): http://www.cisco.com/en/US/products/sw/voicesw/tsd_products_support_category_home.html

# Maintenance

The following sections describe phone maintenance.

## Cisco Unified IP Conference Phone Reset or Restore

The following sections describe the methods for resetting or restoring the conference phone.

### Settings Reset

A factory reset provides a way to recover if the conference phone experiences an error. The **Reset Settings** menu on the device has three options:

- All
- Network

- Security

You can reset a conference phone at any time after the conference phone has started up.

To reset the device, press **Apps** > **Admin Settings** > **Reset Settings**, then select one of the following settings to reset back to factory defaults:

- All
- Network
- Security

# Quality Report Tool

The Quality Report Tool (QRT) is a voice quality and general problem-reporting tool for the conference phone. The QRT feature is installed as part of Cisco Unified Communications Manager.

You can configure users' conference phones with QRT. When you do so, users can report problems with conference phone calls by pressing the QRT softkey. This softkey is available only when the conference phone is in the Connected, Connected Conference, Connected Transfer, or OnHook states.

When a user presses the QRT softkey, a list of problem categories appears. The user selects the appropriate problem category and this feedback is logged in an XML file. Actual information logged depends on the user selection and whether the destination device is a conference phone.

For more information about using QRT, see the *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, conference phones use these statistical metrics that are based on concealment events. The DSP plays concealment frames to mask frame loss in the voice packet stream.

- Concealment Ratio metrics: Show the ratio of concealment frames over total speech frames. An interval conceal ratio is calculated every 3 seconds.
- Concealed Second metrics: Show the number of seconds in which the DSP plays concealment frames due to lost frames. A severely "concealed second" is a second in which the DSP plays more than five percent concealment frames.
- MOS-LQK metrics: Use a numeric score to estimate the relative voice listening quality. The conference phone calculates the mean opinion score (MOS) for listening quality (LQK) based audible concealment events due to frame loss in the preceding 8 seconds, and includes perceptual weighting factors such as codec type and frame size.

MOS LQK scores are produced by a Cisco proprietary algorithm that is an implementation of P.VTQ, an ITU provisional standard.

**Note** Concealment ratio and concealment seconds are primary measurements based on frame loss while MOS LQK scores project a “human-weighted” version of the same information on a scale from 5 (excellent) to 1 (bad) for measuring listening quality.

Listening quality scores (MOS LQK) relate to the clarity or sound of the received voice signal. Conversational quality scores (MOS CQ such as G.107) include impairment factors, such as delay, that degrade the natural flow of conversation.

For information about configuring voice quality metrics for conference phones, see the *Cisco Unified Communications Manager System Guide*, “Cisco Unified IP Phones” chapter, “Phone Features” section.

You can access voice quality metrics from the conference phone by using the Call Statistics screen or remotely by using Streaming Statistics.

To use the metrics for monitoring voice quality, note the typical scores under normal conditions of zero packet loss, and use the metrics as a baseline for comparison.

It is important to distinguish significant changes from random changes in metrics. Significant changes are scores that change about 0.2 MOS or greater and persist in calls that last longer than 30 seconds. Conceal Ratio changes should indicate greater than 3 percent frame loss.

MOS LQK scores can vary based on the codec that the conference phone uses. The following codecs provide these maximum MOS LQK scores under normal conditions with zero frame loss:

- G.711 codec gives 4.5 score
- G.719A/ AB gives 3.7 score

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

When you observe significant and persistent changes to metrics, use the following table for general troubleshooting information.

*Table 38: Changes to Voice Quality Metrics*

| Metric Change | Condition |
|---|---|
| MOS LQK scores decrease significantly | Network impairment from packet loss or high jitter:<br>• Average MOS LQK decreases could indicate widespread and uniform impairment.<br>• Individual MOS LQK decreases indicate bursty impairment.<br>Cross-check with Conceal Ratio and Conceal Seconds for evidence of packet loss and jitter. |
| MOS LQK scores decrease significantly | • Check to see if the conference phone is using a different codec than expected (RxType and TxType).<br>• Check to see if the MOS LQK version changed after a firmware upgrade. |

| Metric Change | Condition |
|---|---|
| Conceal Ratio and Conceal Seconds increase significantly | Network impairment from packet loss or high jitter. |
| Conceal Ratio is near or at zero, but the voice quality is poor | • Noise or distortion in the audio channel such as echo or audio levels.<br>• Tandem calls that undergo multiple encode/decode such as calls to a cellular network or calling card network.<br>Check packet transmit (TxCnt) and packet receive (RxCnt) counters to verify that voice packets are flowing. |

**Note** Voice quality metrics do not account for noise or distortion, only frame loss.

**Related Topics**

Call Statistics Screen, on page 108

Remote Monitoring, on page 111

# Cisco Unified IP Phone Cleaning

To clean your conference phone, use a soft, dry cloth to wipe the conference phone and the LCD screen. Do not apply liquids or powders directly on the conference phone. As with all non-weather-proof electronics, liquids and powders can damage the components and cause failures.

APPENDIX A

# Internal Support Website

## Internal Support Website Overview

If you are an administrator, you are likely the primary source of information for conference phones in your network or company. It is important to provide current and thorough information about the conference phone to end users.

We recommend that you create a web page on your internal support site that provides end users with important information about the conference phone.

## Phone User Support

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

## IP Phone Manuals

You should provide end users with access to user documentation for the conference phones. Each conference phone user guide includes detailed user instructions for key conference phone features.

There are several conference phone models available, so to assist users in finding the appropriate documentation on the Cisco website, Cisco recommends that you provide links to the current documentation. If you do not want to or cannot send users to the Cisco website, Cisco suggests that you download the PDF or epub files and provide them to end users on your website.

For a list of available documentation, go to the conference phone website at this URL: http://www.cisco.com/en/US/products/ps12965/index.html.

# IP Phone Features User Subscription and Setup

End users can perform a variety of activities using Cisco Unified Communications Manager Self Care Portal. These activities include subscribing to services, setting up call forwarding numbers, configuring ring settings, and creating a personal address book. Keep in mind that configuring settings on a conference phone using a website might be new for your end users. You need to provide as much information as possible to ensure that they can successfully access and use the Cisco Unified Communications Manager Self Care Portal.

Make sure to provide end users with the following information:

- 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, and *portnumber* is the port number of the web server.
- A user ID, default password, and default PIN are needed to access the application.

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

You can also refer users to Cisco Unified IP Conference Phone 8831 User Guide for Cisco Unified Communications Manager, which is available at this URL: http://www.cisco.com/en/US/products/ps12965/products_user_guide_list.html.

# User Voice Messaging System Access

Cisco Unified Communications Manager lets you integrate with many different voice mail 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 mail messaging system account.
- 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.

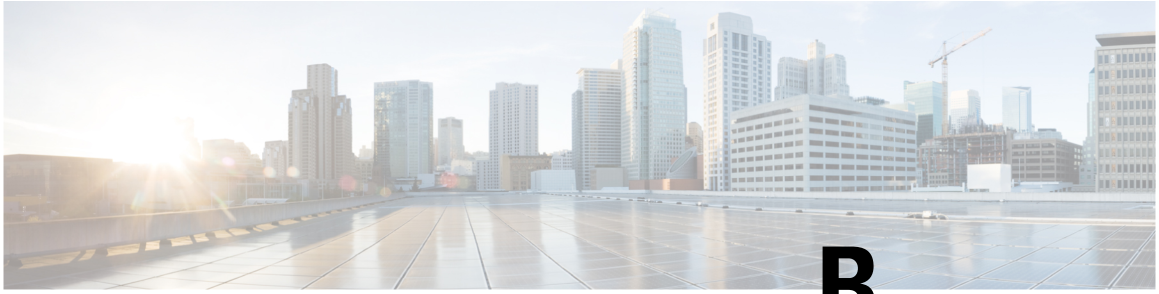
# User Personal Directory Entries Setup

Users can configure personal directory entries on the conference phone. To configure personal directory, users must have access to Cisco Unified Communications Manager Self Care Portal.

**Note** Cisco Unified IP Conference Phone does not support address book synchronization with the Cisco IP Phone Address Book Synchronizer.

### Related Topics

IP Phone Features User Subscription and Setup, on page 140



APPENDIX B

# International User Support

## Localization Support

Translated and localized versions of the conference phone are available in several languages. If you are supporting conference phones in a non-English environment, see the following sections to ensure that the phones are set up properly for your users.

## Language Overlays for Phone Buttons

To support the needs of international users, the button labels on the conference phones exhibit icons rather than text to indicate the purposes of the buttons. You can purchase language-specific text overlays to add to a conference phone. To order these language-specific overlays, go to this website: http://www.overlaypro.com/cisco/.

**Note** Phone overlays are available only for languages in which conference phone software has been localized. All languages may not be immediately available, so continue to check the website for updates.

## Unified Communications Manager Endpoints Locale Installer

By default, Cisco IP Phones are set up for the English (United States) locale. To use the Cisco IP Phones in other locales, you must install the locale-specific version of the Unified Communications Manager Endpoints Locale Installer on every Cisco Unified Communications Manager server in the cluster. The Locale Installer installs the latest translated text for the phone user interface and country-specific phone tones on your system so that they are available for the Cisco IP Phones.

To access the Locale Installer required for a release, access https://software.cisco.com/download/navigator.html?mdfid=286037605&flowid=46245, navigate to your phone model, and select the Unified Communications Manager Endpoints Locale Installer link.

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

**Note** The latest Locale Installer may not be immediately available; continue to check the website for updates.

APPENDIX C

# Technical Specifications

## Physical and Operating Environment Specifications

| Specification | Value or Range |
|---|---|
| Operating Temperature | 0°C to 40°C (32° to 104°F) |
| Operating Relative Humidity | 10 to 95% (noncondensing) |
| Storage Temperature | 14 to 140°F (-10 to 60°C) |
| Operating Altitude | -500 to 6,500 ft. (de-rate 1°C per 1000 ft.) |
| Dimensions<br>(HxWxD) | • Base: 10.38 x 10.38 x 2.0 in. (15.05 x 26.35 x 5.08 cm)<br>• Control panel: 5.75 x 5.0 x 1.0 in. (14.61 x 12.7 x 2.54 cm)<br>• Microphones: 3.5 x 2.5 x 0.5 in. (8.89 x 6.35 x 1.27 cm)<br>• Charger tray: 6.5 x 4.5 x 0.75 in. (16.51 x 11.43 x 1.90 cm) |
| Weight | • Base 3.50 lbs. (1,587.0 grams)<br>• DCU 0.56 lbs. (253.0 grams)<br>• Wired Microphones 0.15 lbs. (66.8 grams)<br>• Wireless Microphones 0.14 lbs. (64.7 grams)<br>• Charger 0.42 lbs. (191.9 grams) |
| Display | 3.25 x 1.5 in. (8.26 x 3.81 cm); 396 x 162 pixels |

| Specification | Value or Range |
|---|---|
| Power | • AC/DC adapter (100-240 V~, 50-60 Hz, 500 mA)<br>• Power over Ethernet (48 V, 380 mA)<br>• Power interface cable |
| Conference Room Coverage | • 20 ft. by 20 ft Sound Base only<br>• 20 ft by 30 ft (Sound Base + Extension Microphone Kit)<br>• > 30 ft by 40 ft (Two Sound Bases connected in Linked mode)<br>**Note** The Cisco Unified IP Conference Phone 8831 supports wired and wireless microphones. The Cisco Unified IP Conference Phone 8831NR supports only wired microphones. |
| Audio Range | 200Hz to 14kHz (wide band voice support) |
| Loudness | 86.5dB at 0.5 meters |
| Cables | One 25-ft. CAT 5 network cable |
| Cable Distance Requirements | As supported by the Ethernet Specification, each conference phone must be within 100 meters (330 feet) of a wiring closet. |

# Cable Specifications

The conference phone has the following cabling requirements:

- RJ-45 plug for the 25-ft. CAT 5 cable connection on the bottom of the conference phone
- RJ-45 plug for the 25-ft. CAT 5 cable connection on the power interface cable
- 6-ft., 48-volt connector to the power interface cable
- (Optional) 25-ft Daisy chain connection cable for use with Linked Mode.

# Phone Behavior During Times of Network Congestion

Anything that degrades network performance can affect phone audio and, in some cases, can cause a call to drop. Sources of network degradation can include, but are not limited to, the following activities:

- Administrative tasks, such as an internal port scan or security scan

- Attacks that occur on your network, such as a Denial of Service attack

APPENDIX D

# Basic Phone Administration Steps

## Phone Administration Overview

This section 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 these tasks. They are 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 have already been done and are in place for existing users.

## 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 describes 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's phone by following these steps.

### Procedure

**Step 1** Log onto Cisco Unified Communications Manager Administration.

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

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

**Step 4** Select on the LDAP directory name.

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

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

**Step 6** Proceed to Identify Phone, on page 151.

## Add User Directly to Cisco Unified Communications Manager

If you are not using an LDAP directory, you can add a user directly to Cisco Unified Communications Manager Administration by following these steps:

### Procedure

**Step 1** Choose **User Management** > **End User**, then select **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** Select **Save**.

**Step 4** Proceed to the section Identify Phone, on page 151.

# Identify Phone

To configure the phone, you must first identify the phone and then configure it 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, perform 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 on the phone.

  Make sure that the value comprises 12 hexadecimal characters.

  **Example:** 00127F576611 (MAC address on john doe's phone)

- Description: This is an optional field in which you can enter a useful description, such as *john doe's phone*. This will help you if you need to search on information about this user.
- Device Pool: Choose the device pool to which you want this phone assigned. 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 on 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 (for example, line, call park) is used for each button.

  Phone button templates are defined on 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 the **Find** button to find all configured phone button templates and their current settings.

- Softkey Template: Choose the appropriate softkey template. The softkey template determines the configuration of the softkeys on Cisco Unified IP Phones. Leave this field blank if the common device configuration contains the assigned softkey template.

  Softkey templates are defined on the Softkey Template Configuration window of Cisco Unified Communications Manager Administration (**Device** > **Device Settings** > **Softkey Template**). You can use the search fields in conjunction with the **Find** button to find all configured softkey templates and their current settings.

- Common Phone Profile: From the drop-down list box, choose a common phone profile from the list of available common phone profiles.

  Common Phone Profiles are defined on 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 the **Find** button to find all configured common phone profiles and their current settings.

- Calling Search Space: From the drop-down list box, 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.

  Calling Search Spaces are defined on 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 the **Find** button 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 menu, choose the user ID of the assigned phone user.

b) In the Protocol Specific Information pane 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 it to the phone. If the phone does not support security, choose a nonsecure profile.

To identify the settings that are contained in the profile, choose **System** > **Security Profile** > **Phone Security Profile**.

The security profile chosen should be based on the overall security strategy of the company.

c) In the Extension Information pane of this window, check the Enable Extension Mobility box if this phone supports Cisco Extension Mobility.
d) Select **Save**.

**Step 2** Configure line settings:

a) On the Phone Configuration window, select 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.

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

**Example:** 26640 is the directory number of user John Doe in the example above.

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 pane 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 pane 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 be forwarded to the voice mail for this line, check the Voice Mail box next to the Forward Busy Internal and Forward Busy External items in the left column of the Call Pickup and Call Forward Settings pane.

f) In the Line 1 on Device... pane of 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 will be displayed 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 numbers 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 example above, 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 select the **Propagate Selected** button. (The check box at right displays only if other devices share this directory number.)

g) Select **Save**.
h) Select **Associate End Users** at the bottom of the window to associate a user to the line being configured. Use the Find button in conjunction with the Search fields to locate the user, then check the box next to

the user's name, then choose **Add Selected**. The user's name and user ID should now appear in the Users Associated With Line pane of the Directory Number Configuration window.

i) Select **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 the Find button to locate the user you have added (for example, *doe* for the last name).
- Select the user ID (for example, *johndoe*). The End User Configuration window appears.
- Select **Device Associations**.
- Use the Search fields and the Find button to locate the device with which you want to associate to the user. Select the device, then choose **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 154.

# Perform Final End User Configuration Steps

If you are not already in 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**.