



## **Cisco Unified IP Phone 8941 and 8945 Administration Guide for Cisco Unified Communications Manager 10.0 (SCCP and SIP)**

**First Published:** 2014-01-09

**Last Modified:** 2017-05-02

### **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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2018 Cisco Systems, Inc. All rights reserved.



## CONTENTS

---

### Preface

#### Preface xi

Overview xi

Audience xi

Guide Conventions xi

Related Documentation xiii

Cisco Unified IP Phone 8900 Series Documentation xiii

Cisco Unified Communications Manager Documentation xiii

Cisco Business Edition 5000 Documentation xiii

Documentation, Support, and Security Guidelines xiii

Cisco Product Security Overview xiii

---

### PART I

#### About Cisco Unified IP Phone 1

---

### CHAPTER 1

#### Technical Details 3

Physical and Operating Environment Specifications 3

Cable Specifications 4

Network and Computer Port Pinouts 4

Network Port Connector 4

Computer Port Connector 5

Phone Power Requirements 6

Power Outage 8

Power Reduction 8

Network Protocols 8

VLAN Interaction 14

Cisco Unified Communications Manager Interaction 15

Cisco Unified Communications Manager Express Interaction 15

External Devices 16

Phone Behavior During Times of Network Congestion 16

---

## CHAPTER 2

### Cisco Unified IP Phone Hardware 17

Cisco Unified IP Phone Hardware Overview 17

Cisco Unified IP Phone 8941 17

Phone Connections 18

Cisco Unified IP Phone 8945 19

Phone Connections 19

Buttons and Hardware 20

Terminology Differences 23

---

## PART II

### Cisco Unified IP Phone Installation 25

---

## CHAPTER 3

### Cisco Unified IP Phone Installation 27

Verify Network Setup 27

Enable Autoregistration for Phones 28

Install Cisco Unified IP Phone 29

Set Up Phone from Setup Menus 30

Apply a Phone Password 31

Text Menu Entry from Phone 31

Configure Network Settings 32

Set Up IPv4 34

Set Domain Name Field 36

Set Admin VLAN ID Field 36

Set PC VLAN Field 37

Set SW Port Setup Field 37

Set PC Port Setup Field 37

Set DHCP Field 37

Set IP Address Field 38

Set Subnet Mask Field 38

Set Default Router Field 38

Set DNS Server Fields 39

Set Alternate TFTP Field 39

Set TFTP Server 1 Field 39

Set TFTP Server 2 Field 40

Set Secondary Load Server	40
Set DHCP Address Released Field	40
Phone Startup Process	40
Configure Phone Services for Users	41

---

**CHAPTER 4**
**Cisco Unified Communications Manager Phone Setup 43**

Determine the Phone MAC Address	43
Set Up Cisco Unified IP Phone	44
Phone Addition Methods	47
Add Phones Individually	47
Add Phones with a BAT Phone Template	48
Add Users to Cisco Unified Communications Manager	48
Add a User from an External LDAP Directory	49
Add a User Directly to Cisco Unified Communications Manager	49
Add a User to an End User Group	50
Associate Phones with Users	51
Survivable Remote Site Telephony	51
Set Up Cisco Unified Communications Manager Features	54

---

**CHAPTER 5**
**Self Care Portal Management 57**

Self Care Portal Overview	57
Set Up User Access to the Self Care Portal	57
Customize the Self Care Portal Display	58

---

**PART III**
**Hardware and Accessory Installation 59**


---

**CHAPTER 6**
**Cisco Unified IP Phone Accessories 61**

Connect Footstand	61
Handset	62
Headsets	63
Audio Quality	63
Wired Headsets	63
Connect Wired Headset	64
Disable a Wired Headset	64
Bluetooth Wireless Headsets	64

Enable a Bluetooth Wireless Headset	64
Wireless Headset Using Headset Port	65

---

**PART IV**


---

**Cisco Unified IP Phone Administration 67**


---

**CHAPTER 7**
**Cisco Unified IP Phone Security 69**

View Current Security Features on Phone	69
View Security Profiles	69
Supported Security Features	70
Supported TLS and Ciphers	73
Set Up Locally Significant Certificate	73
Phone Call Security	74
Secure Phone Call Identification	74
Secure Conference Call Identification	75
Provide Encryption for Barge	76
802.1X Authentication	76
Access 802.1X Authentication	77
802.1X Authentication Options	77
Set Device Authentication Field	78
Set EAP-MD5 Fields	78

---

**CHAPTER 8**
**Cisco IP Phone Customization 79**

Custom Phone Rings	79
Set Up Custom Phone Ring	79
Custom Ring File Formats	80
Custom Background Images	81
Set Up Custom Background Image	81
Custom Background File Formats	82
Phone Customization Tools	83
Set Up Idle Display	83

---

**CHAPTER 9**
**Phone Features and Setup 85**

Phone Features and Setup Overview	86
Cisco IP Phone User Support	86
Telephony Features	86

Feature Support by Protocol	108
Phone Button Templates	115
Modify Phone Button Template	116
Set Up PAB or Speed Dial as IP Phone Service	116
Modify Phone Button Template for PAB or Fast Dial	117
Set Up Softkey Template	117
Control Phone Web Page Access	120
Calling Party Normalization	121
Schedule Power Save for Cisco IP Phone	121
Disable Speakerphone	123
Enable Agent Greeting	123
Set Up Automatic Port Synchronization	124
Set Up Do Not Disturb	124
Enable Device Invoked Recording	125
Enable BLF for Call Lists	125
Set Up Call Forward Notification	126
Set Up Incoming Call Toast Timer	127
Set Up Remote Port Configuration	127
Set Up SSH Access	128
Client Matter Codes and Forced Authorization Codes	128
Set Up Phone Minimum Ring Volume	129
Set Up Video Capability	129
Set Up Peer Firmware Sharing	130
Set Auto Save Volume	131

---

**CHAPTER 10**
**Corporate and Personal Directory Setup 133**

Corporate Directory Setup	133
Personal Directory Setup	133
User Personal Directory Entries Setup	134
Download Cisco IP Phone Address Book Synchronizer	134
Cisco IP Phone Address Book Synchronizer Deployment	134
Install Synchronizer	135
Set Up Synchronizer	135

---

**PART V**
**Cisco Unified IP Phone Troubleshooting 137**

---

**CHAPTER 11****Monitoring Phone Systems 139**

- Cisco Unified IP Phone Status 139
  - Display Phone Information Window 139
    - Model Information Fields 140
  - Display Status Menu 140
    - Display Status Messages Window 141
      - Status Messages 141
  - Display Network Statistics Window 146
    - Network Statistics Fields 146
  - Display Call Statistics Window 148
    - Call Statistics Fields 148
- Cisco IP Phone Web Page 150
  - Access Web Page for Phone 150
    - Device Information 151
    - Network Setup 152
    - Network Statistics 157
      - Ethernet Information Web Page 157
      - Access Area and Network Area Web Pages 157
  - Device Logs 158
  - Streaming Statistics 159

---

**CHAPTER 12****Troubleshooting 165**

- General Troubleshooting Information 165
- Startup Problems 167
  - Cisco IP Phone Does Not Go Through the Normal Startup Process 167
  - Cisco IP Phone Does Not Register with Cisco Unified Communications Manager 168
    - Phone Displays Error Messages 168
    - Phone Displays Message: Unprovisioned 168
    - Phone Cannot Connect to TFTP Server or to Cisco Unified Communications Manager 169
    - Phone Cannot Connect to TFTP Server 169
    - Phone Cannot Connect to Server 169
    - Phone Cannot Connect Using DNS 169



Cisco Unified Communications Manager and TFTP Services Are Not Running	170
Configuration File Corruption	170
Cisco Unified Communications Manager Phone Registration	170
Cisco IP Phone Cannot Obtain IP Address	171
Phone Reset Problems	171
Phone Cannot Connect to LAN	171
Phone Resets Due to Intermittent Network Outages	171
Phone Resets Due to DHCP Setting Errors	172
Phone Resets Due to Incorrect Static IP Address	172
Phone Resets During Heavy Network Usage	172
Phone Resets Due to Intentional Reset	172
Phone Resets Due to DNS or Other Connectivity Issues	173
Phone Does Not Power Up	173
Cisco IP Phone Security Problems	173
CTL File Problems	173
Authentication Error, Phone Cannot Authenticate CTL File	173
Phone Cannot Authenticate CTL File	174
CTL File Authenticates but Other Configuration Files Do Not Authenticate	174
Phone Does Not Register	174
Signed Configuration Files Are Not Requested	174
802.1X Authentication Problems	175
802.1X Enabled on Phone but Phone Does Not Authenticate	176
802.1X Not Enabled	176
Factory Reset of Phone Has Deleted 802.1X Shared Secret	176
Audio and Video Problems	177
Phone Display Is Wavy	177
No Speech Path	177
Choppy Speech	177
Poor Audio Quality with Calls that Route Outside Cisco Unified Communications Manager	178
Insufficient Bandwidth for Video Calls	178
Video Changes Resolution	178
General Telephone Call Problems	179
VPN-Connected Phone Does Not Log Calls	179
Phone Call Cannot Be Established	179

Phone Does Not Recognize DTMF Digits or Digits Are Delayed	180
Troubleshooting Procedures	180
Set Up Remote Phone	180
Check TFTP Settings	181
Check DHCP Settings	181
Verify DNS Settings	182
Create a New Phone Configuration File	182
Determine DNS or Connectivity Issues	183
Identify 802.1X Authentication Problems	183
Start Service	184
Control Debug Information from Cisco Unified Communications Manager	184

---

**CHAPTER 13**
**Maintenance 187**

Basic Reset	187
Reset the Phone to the Factory Settings from the Phone Keypad	188
Perform Factory Reset from Phone Menu	188
Perform Network Configuration Reset	188
Remove CTL File	189
Voice Quality Monitoring	189
Voice Quality Troubleshooting Tips	190
Voice Quality Metrics	190
Video Metrics	191
Cisco IP Phone Cleaning	192

---

**CHAPTER 14**
**International User Support 193**

Unified Communications Manager Endpoints Locale Installer	193
International Call Logging Support	193
Language Limitation	194



## Preface

---

- [Overview](#), page xi
- [Audience](#), page xi
- [Guide Conventions](#), page xi
- [Related Documentation](#), page xiii
- [Documentation, Support, and Security Guidelines](#), page xiii

## Overview

*Cisco Unified IP Phone 8941 and 8945 Administration Guide for Cisco Unified Communications Manager (SCCP and SIP)* provides the information you need to understand, install, configure, manage, and troubleshoot the phones on a Voice-over-IP (VoIP) network.

Because of the complexity of an IP telephony network, this guide does not provide complete and detailed information for procedures that you need to perform in Cisco Unified Communications Manager (Cisco Unified CM) or other network devices. See [Documentation, Support, and Security Guidelines](#), on page xiii.

## Audience

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

## Guide Conventions

This document uses the following conventions:

Convention	Description
<b>boldface font</b>	Commands and keywords are in <b>boldface</b> .

Convention	Description
<i>italic font</i>	Arguments for which you supply values are in <i>italics</i> .
[ ]	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 <code>screen font</code> .
input font	Information you must enter is in <code>input font</code> .
<i>italic screen font</i>	Arguments for which you supply values are in <i>italic screen font</i> .
^	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

## Related Documentation

Use the following sections to obtain related information.

### Cisco Unified IP Phone 8900 Series Documentation

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

<https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8900-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>

## Documentation, Support, and Security Guidelines

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

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

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

### Cisco Product Security Overview

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

Further information regarding U.S. export regulations can be found at <https://www.bis.doc.gov/policiesandregulations/ear/index.htm>.



## PART

# About Cisco Unified IP Phone

- [Technical Details, page 3](#)
- [Cisco Unified IP Phone Hardware, page 17](#)







## CHAPTER

# 1

## Technical Details

- [Physical and Operating Environment Specifications, page 3](#)
- [Cable Specifications, page 4](#)
- [Phone Power Requirements, page 6](#)
- [Network Protocols, page 8](#)
- [VLAN Interaction, page 14](#)
- [Cisco Unified Communications Manager Interaction, page 15](#)
- [Cisco Unified Communications Manager Express Interaction, page 15](#)
- [External Devices, page 16](#)
- [Phone Behavior During Times of Network Congestion, page 16](#)

## Physical and Operating Environment Specifications

The following table shows the physical and operating environment specifications for the Cisco Unified IP Phones 8941 and 8945.

**Table 1: Physical and Operating Specifications**

Specification	Value or range
Operating temperature	32 to 104°F (0 to 40°C)
Operating relative humidity	10 to 95% (noncondensing)
Storage temperature	14 to 140°F (-10 to 60°C)
Dimensions (HxWxD)	9.25 x 4.49 x 10.24 in. (235 x 114 x 260 mm)

Specification	Value or range
Weight	<ul style="list-style-type: none"> <li>• Standard: 2.80 lb (1.27 kg)</li> <li>• Slimline: 2.72 lb (1.235 kg).</li> </ul>
Power	<ul style="list-style-type: none"> <li>• 100-240 VAC, 50-60 Hz, 0.5 A: when using the AC adapter</li> <li>• 48 VDC, 0.2 A: when using the in-line power over the network cable</li> </ul>
Cables	Category 3, 5, or 5e for 10Mbps cables with 4 pairs Category 5 or 5e for 100-Mbps cables with 4 pairs <b>Note</b> Cables have 4 pairs of wires for a total of 8 conductors.
Distance Requirements	As supported by the Ethernet Specification, it is assumed that the maximum cable length between each Cisco Unified IP Phone and the switch is 100 meters (330 feet).

## Cable Specifications

- RJ-9 jack (4-conductor) for handset and headset connection.
- RJ-45 jack for the LAN 10/100BaseT connection (labeled 10/100 SW on the Cisco Unified IP Phone 8941 and 8945).
- RJ-45 jack for a second 10/100BaseT compliant connection (labeled 10/100 PC on the Cisco Unified IP Phone 8941 and 8945).
- 48-volt power connector.

## Network and Computer Port Pinouts

Although both the network and computer (access) ports are used for network connectivity, they serve different purposes and have different port pinouts.

- The network port is labeled `Network` on the phone.
- The computer (access) port is labeled `Computer` on the phone.

### Network Port Connector

The following table describes the network port connector pinouts.

**Table 2: Network Port Connector Pinouts**

Pin Number	Function
1	BI_DA+
2	BI_DA-
3	BI_DB+
4	BI_DC+
5	BI_DC-
6	BI_DB-
7	BI_DD+
8	BI_DD-
<b>Note</b>	BI stands for bidirectional, while DA, DB, DC, and DD stand for Data A, Data B, Data C, and Data D respectively.

## Computer Port Connector

The following table describes the computer port connector pinouts.

**Table 3: Computer (Access) Port Connector Pinouts**

Pin Number	Function
1	BI_DB+
2	BI_DB-
3	BI_DA+
4	BI_DD+
5	BI_DD-
6	BI_DA-
7	BI_DC+
8	BI_DC-
<b>Note</b>	BI stands for bidirectional, while DA, DB, DC, and DD stand for Data A, Data B, Data C, and Data D respectively.

## Phone Power Requirements

The Cisco Unified IP 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 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.

The following table provides guidelines for powering the Cisco Unified IP Phone 8941 and 8945.

**Table 4: Guidelines for Powering the Cisco Unified IP Phone 8941 and 8945**

Power Type	Guidelines
External power: Provided through the CP-PWR-CUBE-3 external power supply.	The Cisco Unified IP Phone 8941 and 8945 use the CP-PWR-CUBE-3 power supply.
External power: Provided through the Cisco Unified IP Phone Power Injector.	The Cisco Unified IP Phone Power Injector may be used with any Cisco Unified IP Phone. Functioning as a midspan device, the injector delivers inline power to the attached phone. The Cisco Unified IP Phone Power Injector is connected between a switch port and the IP Phone, and supports a maximum cable length of 100 m between the unpowered switch and the IP Phone.
PoE power: Provided by a switch through the Ethernet cable attached to the phone.	<p>The Cisco Unified IP Phone 8941 supports IEEE 802.3af Class 1 power on signal pairs and spare pairs.</p> <p>The Cisco Unified IP Phone 8945 supports IEEE 802.3af Class 2 power on signal pairs and spare pairs.</p> <p>To ensure uninterruptible operation of the phone, make sure that the switch has a backup power supply.</p> <p>Make sure that the CatOS or IOS version running on your switch supports your intended phone deployment. Refer to the switch documentation for operating system version information.</p>
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 Phone 8941 and 8945.

The following table provides guidelines for powering the Cisco Unified IP Phone 8941 and 8945.

**Table 5: Guidelines for Powering the Cisco Unified IP Phone 8941 and 8945**

Power Type	Guidelines
External power: Provided through the CP-PWR-CUBE-3 external power supply.	The Cisco Unified IP Phone 8941 and 8945 use the CP-PWR-CUBE-3 power supply.
External power: Provided through the Cisco Unified IP Phone Power Injector.	The Cisco Unified IP Phone Power Injector may be used with any Cisco Unified IP Phone. Functioning as a midspan device, the injector delivers inline power to the attached phone. The Cisco Unified IP Phone Power Injector is connected between a switch port and the IP Phone, and supports a maximum cable length of 100 m between the unpowered switch and the IP Phone.
PoE power: Provided by a switch through the Ethernet cable attached to the phone.	<p>The Cisco Unified IP Phone 8941 supports IEEE 802.3af Class 1 power on signal pairs and spare pairs.</p> <p>The Cisco Unified IP Phone 8945 supports IEEE 802.3af Class 2 power on signal pairs and spare pairs.</p> <p>To ensure uninterruptible operation of the phone, make sure that the switch has a backup power supply.</p> <p>Make sure that the CatOS or IOS version running on your switch supports your intended phone deployment. Refer to the switch documentation for operating system version information.</p>
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 Phone 8941 and 8945.

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

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

Document topics	URL
Cisco Unified IP Phone Power Injector	<a href="http://www.cisco.com/en/US/products/ps6951/index.html">http://www.cisco.com/en/US/products/ps6951/index.html</a>
PoE Solutions	<a href="http://www.cisco.com/en/US/netsol/ns340/ns394/ns147/ns412/index.html">http://www.cisco.com/en/US/netsol/ns340/ns394/ns147/ns412/index.html</a>
Cisco Catalyst Switches	<a href="http://www.cisco.com/en/US/products/hw/switches/index.html">http://www.cisco.com/en/US/products/hw/switches/index.html</a>
Integrated Service Routers	<a href="http://www.cisco.com/en/US/products/hw/routers/index.html">http://www.cisco.com/en/US/products/hw/routers/index.html</a>

Document topics	URL
Cisco IOS Software	<a href="http://www.cisco.com/en/US/products/sw/iosswrel/products_ios_cisco_ios_software_category_home.html">http://www.cisco.com/en/US/products/sw/iosswrel/products_ios_cisco_ios_software_category_home.html</a>

## Power Outage

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

## Power Reduction

You can reduce the amount of energy that the Cisco Unified IP Phone 8941 and 8945 consumes by scheduling when the phone goes into power-save mode. In power-save mode, the backlight on the screen is not lit when the phone is not in use. The phone remains in power-save mode for the scheduled duration or until the user lifts the handset or presses any button. In the Phone Configuration window on Cisco Unified Communications Manager Administration, configure the following parameters.

- Days Backlight Not Active: Specify the days that the backlight remains inactive.
- Backlight on Time: Schedule the time of day that the backlight automatically activates on the days listed in the off schedule.
- Backlight on Duration: Indicates the length of time that the backlight is active after the backlight is enabled by the programmed schedule.
- Backlight Idle Timeout: Defines the period of user inactivity on the phone before the backlight is turned off.

## Network Protocols

Cisco Unified IP Phones support several industry-standard and Cisco network protocols required for voice communication. The following table provides an overview of the network protocols that the Cisco Unified IP Phones 8941 and 8945 support.

**Table 6: Supported Network Protocols on the Cisco Unified IP Phone 8941 and 8945**

Network protocol	Purpose	Usage notes
Bluetooth Wireless Technology	<p>Bluetooth enables low bandwidth wireless connections within a range of 30 feet (10 meters). The best performance is in the 3- to 6-foot (1- to 2-meter) range. Bluetooth wireless technology operates in the 2.4 GHz band which is the same as the 802.11b/g band. There can be a potential interference issues. Cisco recommends that you:</p> <ul style="list-style-type: none"> <li>• Use 802.11a that operates in the 5 GHz band.</li> <li>• Reduce the proximity of other 802.11b/g devices, Bluetooth devices, microwave ovens, and large metal objects.</li> </ul> <p><b>Note</b> Only the Cisco Unified IP Phone 8945 supports Bluetooth.</p>	For more information about using Bluetooth headsets with your Cisco Unified IP Phone, see <a href="#">Bluetooth Wireless Headsets</a> , on page 64.
Bootstrap Protocol (BootP)	BootP enables a network device such as the Cisco Unified IP Phone to discover certain startup information; for example, the phone IP address.	
Cisco Audio Session Tunneling (CAST)	The CAST protocol allows IP phones and associated applications to discover remote endpoints and communicate with them without requiring changes to the traditional signalling components, like Cisco Unified Communications Manager and gateways. The CAST protocol allows separate hardware devices to synchronize related media and allows the PC to be used as a video resource for non-video enabled phones.	
Cisco Discovery Protocol (CDP)	<p>CDP is a device-discovery protocol that runs on all Cisco-manufactured equipment.</p> <p>Using CDP, a device can advertise its existence to other devices and receive information about other devices in the network.</p>	The Cisco Unified IP Phone uses CDP to communicate information such as auxiliary VLAN ID, per port power management details, and Quality of Service (QoS) configuration information with the Cisco Catalyst switch.
Cisco Peer-to-Peer Distribution Protocol (CPPDP)	CPPDP is a Cisco proprietary protocol used to form a peer-to-peer hierarchy of devices. This hierarchy is used to distribute firmware files from peer devices to their neighboring devices.	CPPDP is used by the Peer Firmware Sharing feature. For more information, see <a href="#">Set Up Peer Firmware Sharing</a> , on page 130.

Network protocol	Purpose	Usage notes
Dynamic Host Configuration Protocol (DHCP)	<p>DHCP dynamically allocates and assigns an IP address to network devices.</p> <p>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.</p>	<p>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.</p> <p>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 <i>Cisco Unified Communications Manager System Guide</i>.</p> <p><b>Note</b> If you cannot use option 150, you may try using DHCP option 66.</p>
Hypertext Transfer Protocol (HTTP)	HTTP is the standard way of transferring information and moving documents across the Internet and the web.	Cisco Unified IP Phones use HTTP for XML services, downloading of images and configuration files, and for troubleshooting purposes.
Hypertext Transfer Protocol Secure (HTTPS)	Hypertext Transfer Protocol Secure (HTTPS) is a combination of the Hypertext Transfer Protocol with the SSL/TLS protocol to provide encryption and secure identification of servers.	Web applications with both HTTP and HTTPS support have two URLs configured. Cisco Unified IP Phones that support HTTPS choose the HTTPS URL.



Network protocol	Purpose	Usage notes
IEEE 802.1X	<p>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.</p> <p>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.</p>	<p>The Cisco Unified IP Phone implements the IEEE 802.1X standard by providing support for the following authentication methods: EAP-FAST, EAP-TLS, and EAP-MD5.</p> <p>When 802.1X authentication is enabled on the phone, you should disable the PC port and voice VLAN. For more information, see <a href="#">802.1X Authentication</a>, on page 76.</p>
Internet Protocol (IP)	IP is a messaging protocol that addresses and sends packets across the network.	<p>To communicate using IP, network devices must have an assigned IP address, subnet, and gateway.</p> <p>IP addresses, subnets, and gateways identifications are automatically assigned if you are using the Cisco Unified IP Phone with Dynamic Host Configuration Protocol (DHCP). If you are not using DHCP, you must manually assign these properties to each phone locally.</p>
Link Layer Discovery Protocol (LLDP)	LLDP is a standardized network discovery protocol (similar to CDP) that is supported on some Cisco and third-party devices.	The Cisco Unified IP Phone supports LLDP on the PC port.

Network protocol	Purpose	Usage notes
Link Layer Discovery Protocol-Media Endpoint Devices (LLDP-MED)	LLDP-MED is an extension of the LLDP standard developed for voice products.	<p>The Cisco Unified IP Phone supports LLDP-MED on the SW port to communicate information such as:</p> <ul style="list-style-type: none"> <li>• Voice VLAN configuration</li> <li>• Device discovery</li> <li>• Power management</li> <li>• Inventory management</li> </ul> <p>For more information about LLDP-MED support, see the LLDP-MED and <i>Cisco Discovery Protocol</i> white paper: <a href="http://www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper0900aecd804cd46d.shtml">http://www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper0900aecd804cd46d.shtml</a></p>
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.

Network protocol	Purpose	Usage notes
Session Initiation Protocol (SIP)	SIP is the Internet Engineering Task Force (IETF) standard for multimedia conferencing over IP. SIP is an ASCII-based application-layer control protocol (defined in RFC 3261) that can be used to establish, maintain, and terminate calls between two or more endpoints.	Like other VoIP protocols, SIP 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.  You can configure the Cisco Unified IP Phone to use either SIP or Skinny Client Control Protocol (SCCP). Cisco Unified IP Phones do not support the SIP protocol when the phones are operating in IPv6 address mode.
Skinny Client Control Protocol (SCCP)	SCCP includes a messaging set that allows communications between call control servers and endpoint clients such as IP Phones. SCCP is proprietary to Cisco Systems.	Cisco Unified IP Phone 8941 and 8945 use SCCP, version 20, for call control.
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.

Network protocol	Purpose	Usage notes
Transport Layer Security (TLS)	TLS is a standard protocol for securing and authenticating communications.	When security is implemented, Cisco Unified IP Phones use the TLS protocol when securely registering with Cisco Unified Communications Manager.  For more information, see the <i>Cisco Unified Communications Manager Security Guide</i> .
Trivial File Transfer Protocol (TFTP)	TFTP allows you to transfer files over the network.  On the Cisco Unified IP Phone, TFTP enables you to obtain a configuration file specific to the phone type.	TFTP requires a TFTP server in your network, 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.  For more information, see the Cisco TFTP chapter in the <i>Cisco Unified Communications Manager System Guide</i> .
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.

## VLAN Interaction

The Cisco Unified IP Phone 8941 and 8945 have an internal Ethernet switch, enabling forwarding of packets to the phone, and to the access port and the network port on the back of the phone.

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

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

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

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

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

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

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

## Cisco Unified Communications Manager Interaction

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

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

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



### Note

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

## Cisco Unified Communications Manager Express Interaction

When the Cisco IP Phone works with the Cisco Unified Communications Manager Express (Unified CME), the phones must go into CME mode.

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

The Cisco IP Phones do not support the following actions:

- Transfer: Only supported in the connected call transfer scenario.

- Conference: Only supported in the connected call transfer scenario.
- Join: Supported using the Conference button or hookflash access.
- Hold: Supported using the Hold button.
- Barge: Not supported.
- Direct Transfer: Not supported.
- Select: Not supported.

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

## External Devices

We recommend that you use good-quality external devices that are shielded against unwanted radio frequency (RF) and audio frequency (AF) signals. External devices include headsets, cables, and connectors.

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

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

Cisco cannot guarantee the performance of external devices, cables, and connectors.



### Caution

---

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

---

## Phone Behavior During Times of Network Congestion

Anything that degrades network performance can affect phone voice and video quality, 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



## Cisco Unified IP Phone Hardware

- [Cisco Unified IP Phone Hardware Overview, page 17](#)
- [Cisco Unified IP Phone 8941, page 17](#)
- [Cisco Unified IP Phone 8945, page 19](#)
- [Buttons and Hardware, page 20](#)
- [Terminology Differences, page 23](#)

### Cisco Unified IP Phone Hardware Overview

The Cisco Unified IP Phone 8941 and 8945 provides voice communication over an IP network. The Cisco Unified IP Phone functions much like a digital business phone, allowing you to place and receive phone calls and to access features such as Mute, Hold, Transfer, Speed Dial, Call Forward, and more. In addition, because the phone is connected to your data network, it offers enhanced IP telephony features, including access to network information and services, and customizable features and services.

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



#### Caution

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

### Cisco Unified IP Phone 8941

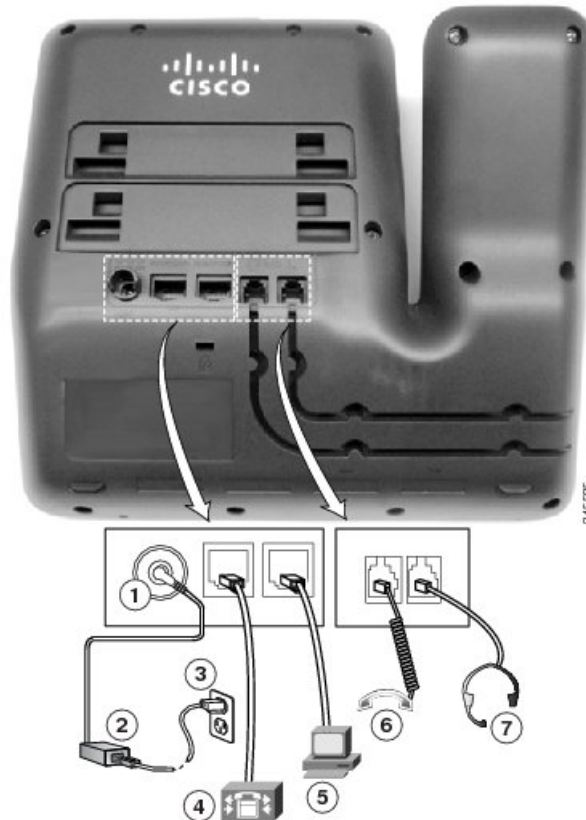
The Cisco Unified IP Phone 8941 provides these features:

- Phone connections
- Footstand
- Buttons and hardware

- Phone screen
- Power-save mode
- Handset rest

## Phone Connections

Use the following figure to help you connect your phone to the corporate IP telephony network.



1	DC adapter port (DC48V)	5	Computer port (10/100 PC) connection
2	AC-to-DC power supply (optional)	6	Handset connection
3	AC power wall plug (optional)	7	Analog headset connection (headset optional)
4	Network port (10/100 SW) with IEEE 802.3af and 802.3at power enabled		



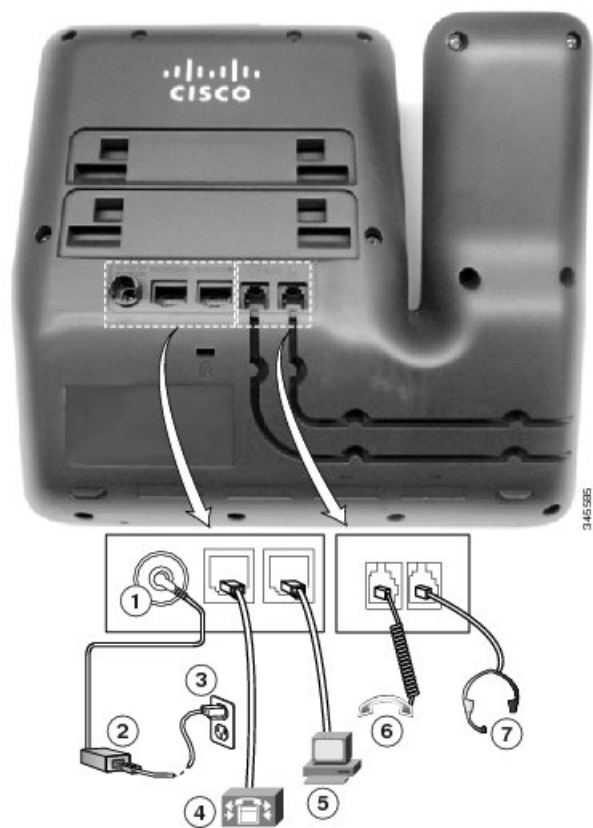
# Cisco Unified IP Phone 8945

The Cisco Unified IP Phone 8945 provides these features:

- Phone connections
- Bluetooth
- Footstand
- Buttons and hardware
- Phone screen
- Power-save mode
- Handset rest

## Phone Connections

Use the following figure to help you connect your phone to the corporate IP telephony network.




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










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






## Buttons and Hardware





Your phone provides quick access to your phone lines, features, and call sessions. The Programmable Feature buttons (left side) are used to view calls on a line or access features such as Speed Dial. These buttons are also called Line buttons.



1	Phone screen	Shows information about your phone, including directory number, call information (for example, caller ID, icons for an active call or call on hold) and available softkeys.
2	Video Camera 	Connects to your Cisco Unified IP Phone and allows you to make a point-to-point video call with another Cisco Unified IP Phone.
3	Lens Cover button	Integrated lens cover protects the camera lens.

4	Softkey buttons 	Allows you to access the softkey options (for the selected call or menu item) that displays on your phone screen.
5	Navigation pad and Select button 	<p>The two-way Navigation pad allows you to scroll through menus, highlight items, and move within a text input field.</p> <p>The Select button (center of the Navigation pad) allows you to select a highlighted item as well as wake up the phone from deep-sleep mode.</p> <p>The Select button is lit (white) when the phone is in power-save mode.</p>
6	Conference button 	Creates a conference call.
7	Hold button 	Places an active call on hold and toggles between an active and on-hold call.
8	Transfer button 	Transfers a call.
9	Redial button 	Redials a call.
10	Keypad 	Allows you to dial phone numbers, enter letters, and choose menu items (by entering the item number).
11	Speakerphone button 	<p>Selects the speakerphone as the default audio path and initiates a new call, picks up an incoming call, or ends a call. During a call, the button is lit green.</p> <p>The speakerphone audio path does not change until a new default audio path is selected (for example, by picking up the handset).</p> <p>If external speakers are connected, the Speakerphone button selects them as the default audio path.</p>
12	Video Mute button 	Mutes the video from the phone screen during a video call. When Video Mute is on, the Video Mute button is lit red.

13	Mute button 	Toggles the microphone on or off during a call. When the microphone is muted, the button is lit red.
14	Headset button 	<p>Selects the headset as the default audio path and initiates a new call, picks up an incoming call, or ends a call. During a call, the button is lit green.</p> <p>A headset icon  in the phone screen header line indicates that the headset is the default audio path. This audio path does not change until a new default audio path is selected (for example, by picking up the handset).</p>
15	Volume button 	<p>Controls the handset, headset, and speakerphone volume (off hook) and controls the ringer volume (on hook).</p> <p>Silences the ringer on the phone if an incoming call is ringing.</p> <p>Your administrator sets a minimum ringer volume level ranging from 0 to 14. The default level is 0 (silent).</p> <p>You can only adjust the ringer volume to a level greater than the configured minimum ring volume value.</p>
16	Messages button 	Autodials voicemail system (varies by system).
17	Applications button 	Opens/closes the Applications menu. Depending on how the phone is set up, use this button to access applications such as Call History, Preferences, and Phone Information.
18	Contacts button 	<p>Opens/closes the Contacts menu. Depending on how the phone is set up, use this button to access Personal Directory, Corporate Directory, or Call History.</p> <p>Use this button to exit from a feature and return to your home screen.</p>
19	Phone Speaker 	Speaker for the phone.

20	Programmable feature buttons (also called Line buttons) 	Each corresponds with a phone line, Speed Dial, and calling feature. Pressing a button for a phone line displays the active calls for that line. Color LEDs indicate the line state: <ul style="list-style-type: none"> <li>• Amber  Ringing call on this line</li> <li>• Green  Active or held call on this line</li> <li>• Red  Shared line in-use remotely</li> </ul> The positions of the feature buttons can be reversed on phones that use a locale with a right-to-left reading orientation, such as Hebrew and Arabic.
21	Handset rest	Provides a rest for the phone handset. When the phone is ringing with an incoming call, the LED in the handset rest flashes red. If there is a new voice message, the LED is lit red.

## Terminology Differences

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

- *Cisco Unified IP Phone 8941 and 8945 User Guide for Cisco Unified Communications Manager (SCCP and SIP)*
- *Cisco Unified IP Phone 8941 and 8945 Administration Guide for Cisco Unified Communications Manager (SCCP and SIP)*
- *Cisco Unified Communications Manager Administration Guide*
- *Cisco Unified Communications Manager System Guide*

User Guide	Administration and System Guides
Speed-Dialing (Placing a call with a speed-dial code)	Abbreviated Dialing
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





## PART II

# Cisco Unified IP Phone Installation

- [Cisco Unified IP Phone Installation, page 27](#)
- [Cisco Unified Communications Manager Phone Setup, page 43](#)
- [Self Care Portal Management, page 57](#)







# Cisco Unified IP Phone Installation

- [Verify Network Setup, page 27](#)
- [Enable Autoregistration for Phones, page 28](#)
- [Install Cisco Unified IP Phone, page 29](#)
- [Set Up Phone from Setup Menus, page 30](#)
- [Configure Network Settings, page 32](#)
- [Phone Startup Process, page 40](#)
- [Configure Phone Services for Users, page 41](#)

## Verify Network Setup

Before you install a phone, you must decide how to configure the phone in your network. Then you can install the phone and verify its functionality.

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



### Note

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

## Procedure

- Step 1** Configure a VoIP Network to meet the following requirements:
- VoIP is configured on your Cisco routers and gateways.
  - Cisco Unified Communications Manager is installed in your network and is configured to handle call processing.
- Step 2** Set up the network to support one of the following:

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

## Enable Autoregistration for Phones

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

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

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

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

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

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

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

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

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

Verify that autoregistration is enabled and is properly configured in Cisco Unified Communications Manager Administration before you connect any Cisco IP Phone to the network. For information about enabling and

configuring autoregistration, see the documentation for your particular Cisco Unified Communications Manager release.

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

### Procedure

- 
- Step 1** In Cisco Unified Communications Manager Administration, click **System > Cisco Unified CM**.
- Step 2** Click **Find** and select the required server.
- Step 3** In **Auto-registration Information**, configure these fields.
- **Universal Device Template**
  - **Universal Line Template**
  - **Starting Directory Number**
  - **Ending Directory Number**
- Step 4** Uncheck the **Auto-registration Disabled on this Cisco Unified Communications Manager** check box.
- Step 5** Click **Save**.
- Step 6** Click **Apply Config**.
- 

### Related Topics

[Phone Addition Methods](#), on page 47

## Install Cisco Unified IP Phone

You must connect the Cisco Unified IP Phone to the network and to a power source before using it. See [Phone Connections](#), on page 18 for the connections for Cisco Unified IP Phone 8941 or [Phone Connections](#), on page 19 for the connections for Cisco Unified IP Phone 8945.



#### Note

Before you install a phone, even if it is new, upgrade the phone to the current firmware image. Before using external devices, read [External Devices](#), on page 16 for safety and performance information.

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

### Procedure

- 
- Step 1** Choose the power source for the phone:
- Power over Ethernet (PoE)
  - External power supply

See [Phone Power Requirements](#), on page 6 for guidelines.

- Step 2** Connect the handset to the Handset port.
- Step 3** (Optional) Connect a headset to the Headset port. You can add a headset later if you do not connect one now. See [Headsets](#), on page 63.
- Step 4** Connect a straight-through Ethernet cable from the switch to the network port labeled Network on the Cisco Unified IP Phone 8941 and 8945. Each Cisco Unified IP Phone ships with one Ethernet cable in the box. You can use either Category 3, 5, or 5e cabling for 10Mbps connections, but you must use Category 5 or 5e for 100 or 1000 Mbps connections. See [Cable Specifications](#), on page 4 for guidelines.
- Step 5** (Optional) Connect a straight-through Ethernet cable from another network device, such as a desktop computer, to the access port labeled Computer on the Cisco Unified IP Phone 8941 and 8945. You can connect another network device later if you do not connect one now. You can use either Category 3, 5, or 5e cabling for 10Mbps connections, but you must use Category 5 or 5e for 100 or 1000 Mbps connections. See [Cable Specifications](#), on page 4 for guidelines.
- Step 6** Monitor the phone startup process. This step adds primary and secondary directory numbers and features that are associated with directory numbers to the phone, and verifies that the phone is configured properly. For more information, see [Phone Startup Process](#), on page 40.
- Step 7** If you are configuring the Ethernet network settings on the phone for an IP network, you can set up an IP address for the phone either by using DHCP or by manually entering an IP address. For more information, see [Set Up Phone from Setup Menus](#), on page 30.
- Step 8** Make calls with the phone to verify that the phone and features work correctly. See the *Cisco Unified IP Phone 8941 and 8945 User Guide for Cisco Unified Communications Manager*.
- Step 9** Provide information to end users about how to use their phones and how to configure their phone options. This step ensures that users have adequate information to successfully use their Cisco Unified IP Phones. For more information, see [Cisco IP Phone User Support](#), on page 86.
- Step 10** Adjust the footstand. For more information, see [Connect Footstand](#), on page 61.
- 

### Related Topics

[Set Up Remote Phone](#), on page 180

## Set Up Phone from Setup Menus

You can control whether a 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 window. The Settings Access field accepts these values:

### Enabled

Allows access to the Settings menu.

### Disabled

Prevents access to the Settings menu.

**Restricted**

Allows access to the User Preferences menu and allows volume changes to be saved. Prevents access to other options on the Settings menu.

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

**Procedure**

- 
- Step 1** Press **Applications**.
- Step 2** Select **Administrator Settings**.
- Note** For information about the Status menu, see [Cisco Unified IP Phone Status, on page 139](#). For information about the Reset Settings menu, see [Basic Reset, on page 187](#).
- Step 3** Enter the password and then press **Select**. The Administrator 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 Administrator 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**.
- 

**Apply a Phone Password**

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


**Procedure**

- 
- Step 1** In Cisco Unified Communications Manager Administration, navigate to the Common Phone Profile Configuration window (**Device > Device Settings > Common Phone Profile**).
- Step 2** Enter a password in the Local Phone Unlock Password option.
- Step 3** Apply the password to the common phone profile that the phone uses.
- 

**Text Menu Entry from Phone**

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 a corresponding number key. Press the key one or more times to display a particular letter. For example, press the **2** key once for “a,” twice quickly for “b,” and three times quickly for “c.” After you pause, the cursor automatically advances to allow you to enter the next letter.
- To enter a period (for example, in an IP address), press star (\*) on the keypad.
- 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 Phone provides several methods you can use to reset or restore option settings, if necessary.

## Configure Network Settings

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

**Table 7: Network Setup Menu Options**

Option	Description	To change
IPv4 Setup	<p>In the IPv4 Setup submenu, you can do the following:</p> <ul style="list-style-type: none"> <li>• Enable or disable the phone to use the IP address that is assign by the DHCP server.</li> <li>• Manually set the IP Address, Subnet Mask, Default Routers, DNS Server, and Alternate TFTP servers.</li> </ul> <p><b>Note</b> You must enter the Alternate TFTP and TFTP server settings when you configure an off-premises phone for SSL VPN to ASA using a built-in client.</p>	<a href="#">Set Up IPv4, on page 34</a>
Host Name	Unique host name assigned to the phone.	Display only—Cannot configure.
Domain Name	Name of the Domain Name System (DNS) domain in which the phone resides.	<a href="#">Set Domain Name Field, on page 36</a>

Option	Description	To change
Operational VLAN ID	<p>Auxiliary Virtual Local Area Network (VLAN) configured on a Cisco Catalyst switch in which the phone is a member.</p> <p>If the phone has not received an auxiliary VLAN, this option indicates the Administrative VLAN.</p> <p>If neither the auxiliary VLAN nor the Administrative VLAN are configured, this option defaults to a VLAN ID of 4095.</p>	<p>Display only—Cannot configure.</p> <p>The phone obtains its Operational VLAN ID using 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.</p>
Admin. VLAN ID	<p>Auxiliary VLAN in which the phone is a member.</p> <p>Used only if the phone does not receive an auxiliary VLAN from the switch; otherwise it is ignored.</p>	<a href="#">Set Admin VLAN ID Field, on page 36</a>
PC VLAN	<p>Allows the phone to interoperate with third-party switches that do not support a voice VLAN. The Admin VLAN ID option must be set before you can change this option.</p>	<a href="#">Set PC VLAN Field, on page 37</a>
SW Port Setup	<p>Speed and duplex of the network port. Valid values are:</p> <ul style="list-style-type: none"> <li>• Auto Negotiate</li> <li>• 1000 Full: 1000-BaseT/full duplex (Supported only for Cisco Unified IP Phone 8945.)</li> <li>• 100 Half: 100-BaseT/half duplex</li> <li>• 100 Full: 100-BaseT/full duplex</li> <li>• 10 Half: 10-BaseT/half duplex</li> <li>• 10 Full: 10-BaseT/full duplex</li> </ul> <p>If the phone is connected to a switch, configure the port on the switch to the same speed/duplex as the phone, or configure both to autonegotiate.</p> <p>If you change the setting of this option, you must change the PC Port Configuration option to the same setting.</p>	<a href="#">Set SW Port Setup Field, on page 37</a>

Option	Description	To change
PC Port Setup	<p>Speed and duplex of the access port. Valid values:</p> <ul style="list-style-type: none"> <li>• Auto Negotiate</li> <li>• 1000 Full: 1000-BaseT/full duplex</li> <li>• 100 Half: 100-BaseT/half duplex</li> <li>• 100 Full: 100-BaseT/full duplex</li> <li>• 10 Half: 10-BaseT/half duplex</li> <li>• 10 Full: 10-BaseT/full duplex</li> </ul> <p>If the phone is connected to a switch, configure the port on the switch to the same speed/duplex as the phone, or configure both to autonegotiate.</p> <p>If you change the setting of this option, you must change the SW Port Configuration option to the same setting.</p>	<a href="#">Set PC Port Setup Field, on page 37</a>
LLDP-MED: Switch Port	<p>Enables and disables Link Layer Discovery Protocol Media Endpoint Discovery (LLDP-MED) on the switch port. Use this setting to force the phone to use a specific discovery protocol, which should match the protocol supported by the switch. Settings include:</p> <ul style="list-style-type: none"> <li>• Enabled (default)</li> <li>• Disabled</li> </ul>	From Cisco Unified Communications Manager Administration, choose <b>Device &gt; Phone &gt; Phone Configuration</b> .

## Procedure

- 
- Step 1** Press **Applications**.
- Step 2** To access the Network Settings menu, select **Administrator Settings > Network Settings**.
- 

## Related Topics

[Text Menu Entry from Phone, on page 31](#)

## Set Up IPv4

The following table describes the IPv4 Setup menu options.



**Table 8: IPv4 Setup Menu Options**

Option	Description	To change
DHCP	Indicates whether the phone has DHCP enabled or disabled.  When DHCP is enabled, the DHCP server assigns the phone an IP address. When DHCP is disabled, you must manually assign an IP address to the phone.	<a href="#">Set DHCP Field, on page 37</a>
IP Address	Internet Protocol (IP) address of the phone.  If you assign an IP address with this option, you must also assign a subnet mask and default router. See the Subnet Mask and Default Router options in this table.	<a href="#">Set IP Address Field, on page 38</a>
Subnet Mask	Subnet mask used by the phone.	<a href="#">Set Subnet Mask Field, on page 38</a>
Default Router 1	Default router used by the phone (Default Router 1).	<a href="#">Set Default Router Field, on page 38</a>
DNS Server 1	Primary Domain Name System (DNS) server (DNS Server 1).	<a href="#">Set DNS Server Fields, on page 39</a>
Alternate TFTP	Indicates whether the phone is using an alternative TFTP server.	<a href="#">Set Alternate TFTP Field, on page 39</a>
Secondary Load Server	A local server or router used by the phone, instead of a designated TFTP server.	<a href="#">Set Secondary Load Server, on page 40</a>
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.  If you set the Alternate TFTP option to yes, you must enter a nonzero value for the TFTP Server 1 option.	<a href="#">Set TFTP Server 1 Field, on page 39</a>
TFTP Server 2	Optional backup TFTP server that the phone uses if the primary TFTP server is unavailable.	<a href="#">Set TFTP Server 2 Field, on page 40</a>
DHCP Address Released	Releases the IP address assigned by DHCP.	<a href="#">Set DHCP Address Released Field, on page 40</a>

### Procedure

---

- Step 1** On the phone, select **Applications**.
  - Step 2** Select **Administrator Settings**.
  - Step 3** Select **Network Setup**.
  - Step 4** Select **IPv4 Setup**.
- 

### Related Topics

[Apply a Phone Password, on page 31](#)  
[Text Menu Entry from Phone, on page 31](#)

## Set Domain Name Field

### Procedure

---

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

## Set Admin VLAN ID Field

### Procedure

---

- Step 1** Scroll to the Admin. VLAN ID option and press **Edit**.
  - Step 2** Enter a new VLAN ID setting.
  - Step 3** Press **Apply**.
  - Step 4** Press **Save**.
-

## Set PC VLAN Field

### Procedure

- 
- Step 1** Ensure that the Admin VLAN ID option is set.
  - Step 2** Scroll to the PC VLAN option and press **Edit**.
  - Step 3** Enter a new PC VLAN setting.
  - Step 4** Press **Apply**.
  - Step 5** Press **Save**.
- 

## Set SW Port Setup Field

### Procedure

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

## Set PC Port Setup Field

### Procedure

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

## Set DHCP Field

### Procedure

- 
- Step 1** Scroll to the DHCP option.
  - Step 2** Press **Edit**.
  - Step 3** Press either **No** to disable DHCP, or press **Yes** to enable DHCP.
-

## Set IP Address Field

### Procedure

---

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

## Set Subnet Mask Field

### Procedure

---

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

## Set Default Router Field

### Procedure

---

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

## Set DNS Server Fields

### Procedure

---

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

## Set Alternate TFTP Field

You must enter the Alternate TFTP and TFTP server fields when you configure an off-premises phone for SSL VPN to ASA using a built-in client.

### Procedure

---

- Step 1** Scroll to the Alternate TFTP option.
  - Step 2** Press **Edit**.
  - Step 3** Press **Yes** if the phone should use an alternative TFTP server.
  - Step 4** Press **No** if the phone should not use an alternative TFTP server.
- 

## Set TFTP Server 1 Field

You must enter the Alternate TFTP and TFTP server fields when you configure an off-premises phone for SSL VPN to ASA using a built-in client.

### Procedure

---

- Step 1** If DHCP is enabled, set the Alternate TFTP option to **Yes**.
  - Step 2** Scroll to the TFTP Server 1 option, press **Select**, and enter a new TFTP server IP address.
  - Step 3** Press **Apply** then press **Save**.
  - Step 4** Erase the security settings.
-

## Set TFTP Server 2 Field

### Procedure

- 
- Step 1** Unlock network configuration options.
  - Step 2** Enter an IP address for the TFTP Server 1 option.
  - Step 3** Scroll to the TFTP Server 2 option, press **Select**, and enter a new backup TFTP server IP address. If there is no secondary TFTP Server, you can use **Delete** to clear the field of a previous value.
  - Step 4** Press **Apply** and then press **Save**.
- 

## Set Secondary Load Server

### Procedure

- 
- Step 1** From Cisco Unified Communications Manager Administration, choose **Device > Phone**.
  - Step 2** Select **Load server**.
  - Step 3** Enter the server hostname or IP address.
- 

## Set DHCP Address Released Field

### Procedure

- 
- Step 1** Scroll to the DHCP Address Released option and press **Edit**.
  - Step 2** Press **Yes** to release the DHCP Address.
- 

## Phone Startup Process

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

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

**Table 9: LED Diagnostic Status**

Hardware test	MWI	Hold	Mute	Speaker
Power is Ready	On	On	On	On
Flash is Accessible	—	On	On	On
RAM Test Successful	—	—	On	On
Ethernet Test Successful	—	—	—	On

- 2 The screen displays the Cisco Systems, Inc., logo screen.
- 3 This message appears as the phone starts up: `Phone not registered`
- 4 The home screen displays:
  - Current date and time
  - Primary directory number
  - Additional directory numbers and speed dial numbers, if configured (only on Cisco Unified IP Phone 8941)
  - Softkeys

If the phone successfully passes through these stages, it has started up properly.

#### Related Topics

[Startup Problems, on page 167](#)

[Cisco IP Phone Does Not Go Through the Normal Startup Process, on page 167](#)

## Configure Phone Services for Users

You can give users access to Cisco IP Phone Services on the IP phone. You can also assign a button to different phone services. These services comprise XML applications and Cisco-signed Java midlets that enable the display of interactive content with text and graphics on the phone. The IP phone manages each service as a separate application. Examples of services include local movie times, stock quotes, and weather reports.

Before a user can access any service:

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

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

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

### Procedure

---

- Step 1** In Cisco Unified Communications Manager Administration, choose **Device > Device Settings > Phone Services**
- Step 2** Verify that your users can access the Cisco Unified Communications Self Care Portal, from which they can select and subscribe to configured services.  
See [Self Care Portal Management](#), on page 57 for a summary of the information that you must provide to end users.
-





# Cisco Unified Communications Manager Phone Setup

---


- [Determine the Phone MAC Address, page 43](#)
- [Set Up Cisco Unified IP Phone, page 44](#)
- [Phone Addition Methods, page 47](#)
- [Add Users to Cisco Unified Communications Manager, page 48](#)
- [Add a User to an End User Group, page 50](#)
- [Associate Phones with Users , page 51](#)
- [Survivable Remote Site Telephony, page 51](#)
- [Set Up Cisco Unified Communications Manager Features, page 54](#)

## Determine the Phone MAC Address

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

### Procedure

Perform one of the following actions:

- On the phone, press **Applications** , select **Phone Information** and look at the MAC Address field.
- Look at the MAC label on the back of the phone.
- Display the web page for the phone and click **Device Information**.

## Set Up Cisco Unified IP Phone

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

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

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

### Procedure

**Step 1** Gather the following information about the phone:

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

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

For more information, see the “Cisco Unified IP Phones” chapter in the *Cisco Unified Communications Manager System Guide*.

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

**Step 3** Customize phone button templates (if required) by changing the number of line buttons, speed-dial buttons or service URL buttons. Select **Device > Device Settings > Phone Button Template** to create and update the templates.

You can add a Privacy or Mobility button to meet user needs.

For more information, see the “Phone button template setup” chapter in the *Cisco Unified Communications Manager Administration Guide* and [Phone Button Templates](#), on page 115.

**Step 4** Define the Device Pools. Select **System > Device Pool**.

Device Pools define common characteristics for devices, such as region, date/time group, softkey template, and MLPP information. For information on Device Pool setup, see the “Device pool setup” chapter in the *Cisco Unified Communications Manager Administration Guide*.

- Step 5** Define the Common Phone Profile. Select **Device > Device settings > Common Phone Profile**. Common phone profiles provide data that the Cisco TFTP server requires, as well as common phone settings, such as Do Not Disturb and feature control options. For more information, see the “Common phone profile setup” chapter in the *Cisco Unified Communications Manager Administration Guide*.
- Step 6** Define a Calling Search Space. In Cisco Unified Communications Manager Administration, click **Call Routing > Class of Control > Calling Search Space**.  
A Calling Search Space is a collection of partitions that are searched to determine how a dialed number is routed. The calling search space for the device and the calling search space for the directory number are used together. The directory number CSS takes precedence over the device CSS. For more information, see the “Calling search space setup” chapter in the *Cisco Unified Communications Manager Administration Guide*.
- Step 7** Configure a security profile for the device type and protocol. Select **System > Security > Phone Security Profile**.  
For more information, see the “Phone security profile setup” chapter in the *Cisco Unified Communications Manager Security Guide*.
- Step 8** Add and configure the phone by completing the required fields in the Phone Configuration window. An asterisk (\*) next to the field name indicates a required field; for example, MAC address and device pool. This step adds the device with the default settings to the Cisco Unified Communications Manager database.  
For more information, see the “Cisco Unified IP Phone Configuration” chapter in the *Cisco Unified Communications Manager Administration Guide*.  
For information about product-specific configuration fields, see the “?” Button Help in the Phone Configuration window.
- Note** If you want to add both the phone and user to the Cisco Unified Communications Manager database at the same time, see the “User/Phone Add Configuration” chapter in the *Cisco Unified Communications Manager Administration Guide*.
- Step 9** Add and configure directory numbers (lines) on the phone by completing the required fields in the Directory Number Configuration window. An asterisk (\*) next to the field name indicates a required field; for example, directory number and presence group. This step adds primary and secondary directory numbers and features associated with directory numbers to the phone.  
For more information, see the “Directory Number Configuration” chapter in the *Cisco Unified Communications Manager Administration Guide*.
- Step 10** Customize softkey templates. Adds, deletes, or changes the order of softkey features that display on the user’s phone to meet feature usage needs.  
For more information, see the *Cisco Unified Communications Manager Administration Guide*, “Softkey Template Configuration” and “Cisco Unified IP Phone Configuration” chapters.
- Step 11** Configure speed-dial buttons and assign speed-dial numbers.  
Users can change speed-dial settings on their phones by using Cisco Unified Communications Self Care Portal.  
For more information, see the “Configuring Speed-Dial Buttons or Abbreviated Dialing” section in the “Cisco Unified IP Phone Configuration” chapter in the *Cisco Unified Communications Manager Administration Guide*.
- Step 12** Configure Cisco Unified IP Phone services and assign services (optional) to provide IP Phone services. Users can add or change services on their phones by using the Cisco Unified Communications Self Care Portal.

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

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

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

**Step 13** Assign services to programmable buttons (optional) to provide access to an IP Phone service or URL. For more information, see the “Adding a Service URL Button” section of the “Cisco Unified IP Phone Configuration” chapter in the *Cisco Unified Communications Manager Administration Guide*.

**Step 14** Add user information by configuring required fields. An asterisk (\*) next to the field name indicates a required field; for example, User ID and last name. This step adds user information to the global directory for Cisco Unified Communications Manager.

**Note** Assign a password (for Self Care Portal) and PIN (for Cisco Extension Mobility and Personal Directory).

For more information, see the “End User Configuration” chapter in the *Cisco Unified Communications Manager Administration Guide*.

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

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

**Step 15** Associate a user to a user group. This step assigns users a common list of roles and permissions that apply to all users in a user group. Administrators can manage user groups, roles, and permissions to control the level of access (and, therefore, the level of security) for system users. For example, you must add users to the standard Cisco CCM End Users group so users can access Cisco Unified Communications Manager User Options.

For more information, see the following sections in the *Cisco Unified Communications Manager Administration Guide*:

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

**Step 16** Associate a user with a phone (optional). This step provides users with control over their phone such as forwarding calls or adding speed-dial numbers or services. Some phones, such as those in conference rooms, do not have an associated user.

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

- Step 17** 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.
- Step 18** In the Directory Number Associations area of the screen, set the primary extension from the drop-down list.
- Step 19** In the Mobility Information area, check the Enable Mobility box.
- Step 20** 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 21** To view all configured user groups, choose **User Management > User Group**.
- Step 22** 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 23** Select **Save**.
- 

### Related Topics

[Phone Displays Message: Unprovisioned, on page 168](#)

## Phone Addition Methods

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

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

Before you add phones individually or with BAT, you need the MAC address of the phone. For more information, see [Determine the Phone MAC Address, on page 43](#).

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

### Related Topics

[Enable Autoregistration for Phones, on page 28](#)

## Add Phones Individually

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

### Procedure

- 
- Step 1** In Cisco Unified Communications Manager Administration, choose **Device > Phone**.
- Step 2** Click **Add New**.
- Step 3** Select the phone type.
- Step 4** Select **Next**.
- Step 5** Complete the information about the phone including the MAC Address.  
For complete instructions and conceptual information about Cisco Unified Communications Manager, see the documentation for your particular Cisco Unified Communications Manager release.
- Step 6** Select **Save**.
- 

## Add Phones with a BAT Phone Template

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

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

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

### Procedure

- 
- Step 1** From Cisco Unified Communications Administration, choose **Bulk Administration > Phones > Phone Template**.
- Step 2** Click **Add New**.
- Step 3** Choose a Phone Type and click **Next**.
- Step 4** Enter the details of phone-specific parameters, such as Device Pool, Phone Button Template, and Device Security Profile.
- Step 5** Click **Save**.
- Step 6** Select **Device > Phone > Add New** to add a phone using the BAT phone template.
- 

## Add Users to Cisco Unified Communications Manager

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

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

- Subscribe to services that are accessible from a Cisco IP Phone.

### Procedure

- 
- Step 1** To add users individually, see [Add a User Directly to Cisco Unified Communications Manager](#), on page 49.
- Step 2** To add users in batches, use the Bulk Administration Tool. This method also enables you to set an identical default password for all users.  
For more information, see the documentation for your particular Cisco Unified Communications Manager release.
- 

## Add a User from an External LDAP Directory

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



### Note

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

### Procedure

- 
- Step 1** Sign into Cisco Unified Communications Manager Administration.
- Step 2** Select **System > LDAP > LDAP Directory**.
- Step 3** Use **Find** to locate your LDAP directory.
- Step 4** Click on the LDAP directory name.
- Step 5** Click **Perform Full Sync Now**.
- 

## Add a User Directly to Cisco Unified Communications Manager

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



### Note

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

### Procedure

- 
- Step 1** From Cisco Unified Communications Manager Administration, choose **User Management > End User**.
- Step 2** Click **Add New**.
- Step 3** In the User Information pane, enter the following:
- **User ID:** Enter the end user identification name. Cisco Unified Communications Manager does not permit modifying the user ID after it is created. You may use the following special characters: =, +, <, >, #, ;, \, , , "" , and blank spaces. **Example:** johndoe
  - **Password and Confirm Password:** Enter five or more alphanumeric or special characters for the end user password. You may use the following special characters: =, +, <, >, #, ;, \, , , "" , and blank spaces.
  - **Last Name:** Enter the end user last name. You may use the following special characters: =, +, <, >, #, ;, \, , , "" , and blank spaces. **Example:** doe
  - **Telephone Number:** Enter the primary directory number for the end user. End users can have multiple lines on their phones. **Example:** 26640 (John Doe's internal company telephone number)
- Step 4** Click **Save**.
- 

## Add a User to an End User Group

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

### Procedure

- 
- Step 1** From Cisco Unified Communications Manager Administration, choose **User Management > User Settings > Access Control Group**.  
The Find and List Users window displays.
- Step 2** Enter the appropriate search criteria and click **Find**.
- Step 3** Select the **Standard CCM End Users** link. The User Group Configuration window for the Standard CCM End Users appears.
- Step 4** Select **Add End Users to Group**. The Find and List Users window appears.
- Step 5** Use the Find User drop-down list boxes to find the users that you want to add and click **Find**.  
A list of users that matches your search criteria appears.
- Step 6** In the list of records that appear, click the check box next to the users that you want to add to this user group. If the list is long, use the links at the bottom to see more results.  
**Note** The list of search results does not display users that already belong to the user group.
- Step 7** Choose **Add Selected**.
-



## Associate Phones with Users

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

### Procedure

- 
- Step 1** From Cisco Unified Communications Manager Administration, choose **User Management > End User**. The Find and List Users window appears.
  - Step 2** Enter the appropriate search criteria and click **Find**.
  - Step 3** In the list of records that appear, select the link for the user.
  - Step 4** Select **Device Association**.  
The User Device Association window appears.
  - Step 5** Enter the appropriate search criteria and click **Find**.
  - Step 6** Choose the device that you want to associate with the user by checking the box to the left of the device.
  - Step 7** Choose **Save Selected/Changes** to associate the device with the user.
  - Step 8** From the Related Links drop-down list in the upper, right corner of the window, select **Back to User**, and click **Go**.  
The End User Configuration window appears and the associated devices that you chose display in the Controlled Devices pane.
  - Step 9** Choose **Save Selected/Changes**.
- 

## Survivable Remote Site Telephony

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

The Detect Unified CM Connection Failure feature determines the sensitivity that the phone has for detecting a connection failure to Cisco Unified Communications Manager (Unified CM), which is the first step before device failover to a backup Unified CM/SRST occurs. Choose one of two options:

- Normal (3 seconds)
- Delayed (6 seconds)

For additional information, see *User Guide for Cisco Prime Unified Provisioning Manager*, "Advanced Setup" chapter.

The following table describes the availability of features during failover.

**Table 10: SRST feature support**

Feature	Supported	Notes
New Call	Yes	
End Call	Yes	
Redial	Yes	
Answer	Yes	
Hold	Yes	
Resume	Yes	
Conference	Yes	
Conference to Active Calls (Join)	No	The Active Calls softkey does not display.
Conference List	No	
Transfer	Yes	
Transfer to Active Calls (Direct Transfer)	No	
Auto Answer	Yes	
Call Waiting	Yes	
Caller ID	Yes	
Audible Message Waiting Indicator	Yes	
Answer Programmable Line Key	Yes	
Unified Session Presentation	No	Conference is the only feature supported due to other feature limitations.
Voicemail	Yes	Voicemail will not be synchronized with other users in the Cisco Unified Communications Manager cluster.

Feature	Supported	Notes
Call Forward All	Yes	Forward state is only available on the phone that sets the forward because there are no shared line appearances in SRST mode. The Call Forward All settings are not preserved on failover to SRST from the Cisco Unified Communications Manager, or from SRST fail-back to the Communications Manager. Any original Call Forward All still active on the Communications Manager should be indicated when the device reconnects to the Communications Manager after failover.
Speed Dial	No	
Service URL Programmable Line Key	Yes	
To Voicemail (iDivert)	No	The iDivert softkey does not display.
Line Filters	Partial	Lines are supported but cannot be shared.
Park Monitoring	No	The Park softkey does not display.
Barge	No	User sees the message That feature is not currently available.
Enhanced Message Waiting Indication	No	Message count badges do not appear on the phone screen. Only the Message Waiting icon displays.
Directed Call Park	No	The softkey does not display.
BLF (Line status)	Yes	
Hold Reversion	No	Calls remain on hold indefinitely.
Remote Hold	No	Calls appear as Local Hold calls.
Meet Me	No	The Meet Me softkey does not display.

Feature	Supported	Notes
PickUp	No	The softkey causes no action.
Group PickUp	No	The softkey causes no action.
Other PickUp	No	The softkey causes no action.
Malicious Call ID	No	The softkey causes no action.
QRT	No	The softkey causes no action.
Hunt Group	No	The softkey causes no action.
Intercom	No	The softkey causes no action.
Mobility	No	The softkey causes no action.
Privacy	No	The softkey causes no action.
Call Back	No	The Call Back softkey does not display.
Video	Yes	
Shared Line	Yes	

## Set Up Cisco Unified Communications Manager Features

Cisco Unified Communications Manager Administration allows you to set some product-specific configuration parameters for Cisco IP Phones.

### Procedure

- Step 1** In Cisco Unified Communications Manager Administration, choose one of the following windows:
- **Device > Phone** (Phone Configuration window) Product Specific Configuration portion of window
  - **Device > Device Settings > Common Phone Profile** (Common Phone Profile Configuration window)
  - **System > Enterprise Phone Configuration** (Enterprise Phone Configuration window)
- Step 2** Click the ? button in Cisco Unified Communications Manager Administration for descriptions of the parameters.
- Step 3** When you set the parameters, check the **Override Common Settings** check box for each setting that you wish to update.  
If you do not check this box, the corresponding parameter setting does not take effect.  
If you set the parameters in the three configuration windows, the setting takes precedence in the following order:

- 1 Phone Configuration window
  - 2 Common Phone Profile window
  - 3 Enterprise Phone Configuration window
-





## Self Care Portal Management

- [Self Care Portal Overview, page 57](#)
- [Set Up User Access to the Self Care Portal, page 57](#)
- [Customize the Self Care Portal Display, page 58](#)

### 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**.
-





## PART

# Hardware and Accessory Installation

- [Cisco Unified IP Phone Accessories, page 61](#)





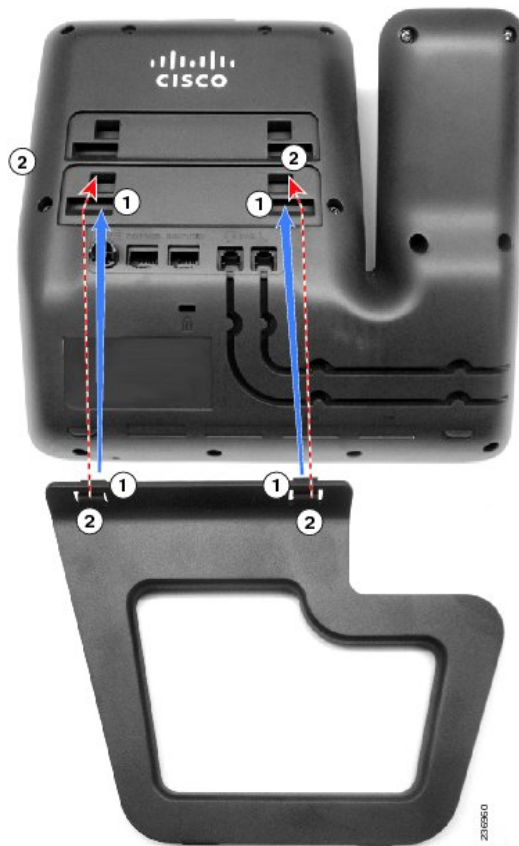
## Cisco Unified IP Phone Accessories

---

- [Connect Footstand, page 61](#)
- [Handset, page 62](#)
- [Headsets, page 63](#)

### Connect Footstand

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



### Procedure

**Step 1** Insert the curved connectors into the lower slots.

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

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

## Handset

The Cisco Unified IP Phone uses a handset that is designed especially for the phone. The handset includes a light strip to indicate incoming calls and voice messages waiting.

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

## Headsets

Although Cisco performs internal testing of third-party headsets for use with the Cisco Unified IP Phones, Cisco does not certify or support products from headset or handset vendors.

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


**Note**

In some cases, hum may be reduced or eliminated by using a local power cube or power injector.

These environmental and hardware inconsistencies in the locations where Cisco Unified IP Phones are deployed means that there is not a single headset solution that is optimal for all environments.

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


**Note**

The Cisco Unified IP Phones 8941 and 8945 support wideband headsets.

### Related Topics

[External Devices, on page 16](#)

## Audio Quality

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

For additional information, see [https://www.cisco.com/c/en/us/products/unified-communications/uc\\_endpoints\\_accessories.html](https://www.cisco.com/c/en/us/products/unified-communications/uc_endpoints_accessories.html)

## Wired Headsets

A wired headset works with all Cisco IP Phone features, including the Volume and Mute buttons. These buttons adjust the earpiece volume and mute the audio from the headset microphone.

When you install a wired headset, make sure you press the cable into the channel in the phone.


**Caution**

Failure to press the cable into the channel in the phone can lead to cable damage.

## Connect Wired Headset

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

### Procedure

- 
- Step 1** Plug the headset into the Headset port on the back of the phone.
  - Step 2** Press the **Headset** button on the phone to place and answer calls using the headset.
- 

## Disable a Wired Headset

You can use Cisco Unified Communications Manager Administration to disable your wired headset and speakerphone.

### Procedure

- 
- Step 1** In Cisco Unified Communications Manager Administration, choose **Device > Phone**.
  - Step 2** In the Find and List Phones window, enter the search criteria for the phone and click **Find**.
  - Step 3** Click the Device Name that you want. The Phone Configuration window is displayed.
  - Step 4** In the Product Specific Configuration Layout portion of the Phone Configuration window, select **Disable Speakerphone and Headset**.
  - Step 5** Click **Save**.
- 

## Bluetooth Wireless Headsets

The Cisco Unified IP Phone 8945 supports Bluetooth Class 2 technology when the headsets support Bluetooth. Bluetooth enables low-bandwidth wireless connections within a range of 30 feet (10 meters). The best performance is in the 3- to 6-foot range (1 to 2 meters). You can pair up to 5 headsets, but only the last one connected is used as the default.



### Note

---

The Cisco Unified IP Phone 8941 does not support Bluetooth.

---

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

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

## Enable a Bluetooth Wireless Headset

Before a user can use a Bluetooth wireless headset, you must enable it.

## Procedure

- 
- Step 1** In Cisco Unified Communications Manager Administration, choose **Device > Phone**.
- Step 2** Locate the phone you want to modify, and go to the Phone Configuration window for that phone.
- Step 3** In the Phone Configuration window, select **Enable** for the Bluetooth setting and **Handsfree** for the Bluetooth Profiles setting.
- Step 4** Save your changes.
- 

## Wireless Headset Using Headset Port

The phone supports a wireless analog headset. To use a wireless headset, users connect a base station to the headset port. The base station communicates with the wireless headset.

The Electronic Hookswitch feature enables users to remotely control basic IP phone functionality from the wireless headset. Basic IP phone functionality includes off-hook and on-hook, ring indication, audio volume control, and mute.

The Electronic Hookswitch feature supports the following headset devices:

- Plantronics
  - Savi and CS5xx series with cable APC-82

For more information about wireless headsets that work in conjunction with the Electronic Hookswitch feature, go to the following URL:

[http://www.cisco.com/en/US/prod/voicesw/ucphone\\_headsets.html](http://www.cisco.com/en/US/prod/voicesw/ucphone_headsets.html)







# PART IV

## Cisco Unified IP Phone Administration

- [Cisco Unified IP Phone Security, page 69](#)
- [Cisco IP Phone Customization, page 79](#)
- [Phone Features and Setup, page 85](#)
- [Corporate and Personal Directory Setup, page 133](#)





## Cisco Unified IP Phone Security

---

- [View Current Security Features on Phone, page 69](#)
- [View Security Profiles, page 69](#)
- [Supported Security Features, page 70](#)

### View Current Security Features on Phone

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

#### Procedure

---

- Step 1** Press **Applications**.
- Step 2** Choose **Administrator Settings > Security Setup**.
- 

### View Security Profiles

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

#### Procedure

---

- Step 1** In Cisco Unified Communications Manager Administration, select **System > Security > Phone Security Profile**.
- Step 2** Look at the Security Mode setting.
-

## Supported Security Features

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

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

The Cisco Unified IP Phone 8941 and 8945 use the Phone security profile, which defines whether the device is nonsecure or encrypted. For information on applying the security profile to the phone, see the *Cisco Unified Communications Manager Security Guide*.

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

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 the *Cisco Unified Communications Manager Security Guide*.

The following table provides an overview of the security features that the Cisco Unified IP Phone 8941 and 8945 support. For more information about these features and about Cisco Unified Communications Manager and Cisco Unified IP Phone security, see *Cisco Unified Communications Manager Security Guide*.

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



### Note

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

**Table 11: Overview of Security Features**

Feature	Description
Image authentication	Signed binary files (with the extension .sgn) prevent tampering with the firmware image before it is loaded on a phone. Tampering with the image causes a phone to fail the authentication process and reject the new image.
Customer-site certificate installation	Each Cisco Unified IP Phone requires a unique certificate for device authentication. Phones include a manufacturing installed certificate (MIC), but for additional security, you can specify 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.

Feature	Description
Device authentication	Occurs between the Cisco Unified Communications Manager server and the phone when each entity accepts the certificate of the other entity. Determines whether a secure connection between the phone and a Cisco Unified Communications Manager should occur and, if necessary, creates a secure signaling path between the entities by using TLS protocol. Cisco Unified Communications Manager does not register phones unless they are authenticated by the Cisco Unified Communications Manager.
File authentication	Validates digitally signed files that the phone downloads. The phone validates the signature to make sure that file tampering did not occur after the file creation. Files that fail authentication are not written to flash memory on the phone and the phone rejects such files without further processing.
Signaling Authentication	Uses the TLS protocol to validate that no tampering has occurred to signaling packets during transmission.
Manufacturing installed certificate	Each Cisco Unified IP Phone contains a unique manufacturing installed certificate (MIC), which is used for device authentication. The MIC is a permanent unique proof of identity for the phone and allows Cisco Unified Communications Manager to authenticate the phone.
Secure SRST reference	After you configure a SRST reference for security and then reset the dependent devices in Cisco Unified Communications Manager Administration, the TFTP server adds the SRST certificate to the phone cnf.xml file and sends the file to the phone. A secure phone then uses a TLS connection to interact with the SRST-enabled router.
Media encryption	Uses SRTP to ensure that the media streams between supported devices prove secure and that only the intended device receives and reads the data. Includes creating a media master key pair for the devices, delivering the keys to the devices, and securing the delivery of the keys while the keys are in transport.
Signaling encryption	Ensures that all SCCP signaling messages sent between the device and the Cisco Unified Communications Manager server are encrypted.
CAPF (Certificate Authority Proxy Function)	Implements parts of the certificate generation procedure that are too processing-intensive for the phone and interacts with the phone for key generation and certificate installation. The CAPF can be configured to request certificates from customer-specified certificate authorities on behalf of the phone or it can be configured to generate certificates locally.
Security profiles	Defines whether the phone is nonsecure or encrypted.
Encrypted configuration files	Lets you ensure the privacy of phone configuration files.
Optional disabling of the web server functionality for a phone	You can prevent access to a phone web page, which displays a variety of operational statistics for the phone.

Feature	Description
Phone hardening	<p>Additional security options, which you control from Cisco Unified Communications Manager Administration:</p> <ul style="list-style-type: none"> <li>• Disabling PC port</li> <li>• Disabling PC Voice VLAN access</li> <li>• Disabling access to web pages for a phone</li> </ul> <p><b>Note</b> You can view current settings for the PC Port Disabled, GARP Enabled, and Voice VLAN enabled options by looking at the phone Security Configuration menu.</p>
802.1X Authentication	The Cisco Unified IP Phone can use 802.1X authentication to request and gain access to the network.

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

The following table describes the options in this menu.

**Table 12: 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 <b>Device &gt; Phone &gt; Phone Configuration</b> .
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 the “Using the Certificate Authority Proxy Function” chapter in <i>Cisco Unified Communications Manager Security Guide</i> .
Trust List	The Trust List provides submenus for CTL signature and Call Manager/TFTP Server.	For more information, see <a href="#">Set Up Locally Significant Certificate</a> , on page 73.
802.1X Authentication	Displays the device authentication, EAP/MD5, and transaction status.	See <a href="#">Set EAP-MD5 Fields</a> , on page 78.

## Related Topics

[Control Phone Web Page Access](#), on page 120

[802.1X Authentication](#), on page 76

## Supported TLS and Ciphers

TLS v1.0

Cipher Suite: TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA (0x0035)

Cipher Suite: TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA (0x002f)

Cipher Suite: TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (0x000a)

## Set Up Locally Significant Certificate

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

### Before You Begin

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

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


For more information, see the *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 **Applications > Administrator Settings > Security Setup**.
- Note** You can control access to the Administrator Settings Menu using the Settings Access field in the Cisco Unified Communications Manager Administration Phone Configuration window. For more information, see the *Cisco Unified Communications Manager Administration Guide*.
- Step 3** To unlock settings, see [Apply a Phone Password](#), on page 31.
- Step 4** Scroll to LSC and press **Update**.  
The phone prompts for an authentication string.
- Step 5** Enter the authentication code and press **Submit**.  
The phone begins to install, update, or remove the LSC, depending on how the CAPF was configured. During the procedure, a series of messages appears in the LSC option field in the Security Configuration menu, so you can monitor progress.
- Step 6** You can verify that an LSC is installed on the phone by choosing **Administrator Settings > Security Setup** and ensuring that the LSC setting shows **Installed**.
-

## Phone Call Security

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

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



### Note

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

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



### Note

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

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

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

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


## Secure Phone Call Identification

A secure call is established when your phone, and the phone on the other end, is configured for secure calling. The other phone can be in the same Cisco IP network, or on a network outside the IP network. Secured calls can only be made between two phones. Conference calls should support secure call after secure conference bridge set up.

A secured call is established using this process:

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



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

**Note**

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

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

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

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


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

**Note**

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

## Secure Conference Call Identification

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

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

**Note**

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.

## Provide Encryption for Barge

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

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

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

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

## 802.1X Authentication

The Cisco IP Phones support 802.1X Authentication.

Cisco IP Phones and Cisco Catalyst switches traditionally use Cisco Discovery Protocol (CDP) to identify each other and determine parameters such as VLAN allocation and inline power requirements. CDP does not identify locally attached workstations. Cisco IP Phones provide an EAPOL pass-through mechanism. This mechanism allows a workstation attached to the Cisco IP Phone to pass EAPOL messages to the 802.1X authenticator at the LAN switch. The pass-through mechanism ensures that the IP phone does not act as the LAN switch to authenticate a data endpoint before accessing the network.

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

Support for 802.1X authentication requires several components:

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

You must perform the following actions to configure 802.1X.


- Configure the other components before you enable 802.1X Authentication on the phone.
- Configure PC Port: The 802.1X standard does not consider VLANs and thus recommends that only a single device should be authenticated to a specific switch port. However, some switches (including Cisco Catalyst switches) support multidomain authentication. The switch configuration determines whether you can connect a PC to the PC port of the phone.

- Enabled: If you are using a switch that supports multidomain authentication, you can enable the PC port and connect a PC to it. In this case, Cisco IP Phones support proxy EAPOL-Logoff to monitor the authentication exchanges between the switch and the attached PC. For more information about IEEE 802.1X support on the Cisco Catalyst switches, see the Cisco Catalyst switch configuration guides at:  
[http://www.cisco.com/en/US/products/hw/switches/ps708/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html)
  - Disabled: If the switch does not support multiple 802.1X-compliant devices on the same port, you should disable the PC Port when 802.1X authentication is enabled. If you do not disable this port and subsequently attempt to attach a PC to it, the switch denies network access to both the phone and the PC.
- Configure Voice VLAN: Because the 802.1X standard does not account for VLANs, you should configure this setting based on the switch support.
    - Enabled: If you are using a switch that supports multidomain authentication, you can continue to use the voice VLAN.
    - Disabled: If the switch does not support multidomain authentication, disable the Voice VLAN and consider assigning the port to the native VLAN.

## Access 802.1X Authentication

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

### Procedure

- 
- Step 1** Press **Applications** .
- Step 2** Choose **Administrator Settings > Security Setup > 802.1X Authentication**.
- Step 3** Configure the options as described in [802.1X Authentication Options](#), on page 77.
- Step 4** To exit this menu, press **Exit**.
- 

## 802.1X Authentication Options

The following table describes the 802.1X authentication options.


**Table 13: 802.1X Authentication Settings**

Option	Description	To change
Device Authentication	Determines whether 802.1X authentication is enabled: <ul style="list-style-type: none"> <li>• Enabled: Phone uses 802.1X authentication to request network access.</li> <li>• Disabled: Default setting. The phone uses CDP to acquire VLAN and network access.</li> </ul>	See <a href="#">Set Device Authentication Field</a> , on page 78.

Option	Description	To change
Transaction Status	<p>State: Displays the state of 802.1x authentication:</p> <ul style="list-style-type: none"> <li>• Disconnected: Indicates that 802.1x authentication is not configured on the phone.</li> <li>• Authenticated: Indicates that the phone is authenticated.</li> <li>• Held: Indicates that the authentication process is in progress.</li> </ul> <p>Protocol: Displays the EAP method that is used for 802.1x authentication (can be EAP-FAST or EAP-TLS).</p>	Display only. Cannot configure.


## Set Device Authentication Field

### Procedure

- 
- Step 1** Press **Applications** .
- Step 2** Choose **Admin settings > Security setup > 802.1X Authentication**
- Step 3** Set the Device Authentication option:
- Yes
  - No
- Step 4** Press **Apply**.
- 

## Set EAP-MD5 Fields

### Procedure

- 
- Step 1** Press **Applications** .
- Step 2** Choose **Administrator Settings > Security Setup > 802.1X Authentication > EAP-MD5**.
- Step 3** To change the shared secret, choose **Shared Secret**.
- Step 4** Enter the shared secret.
- Step 5** Press **Apply**.
-



## Cisco IP Phone Customization

---

- [Custom Phone Rings, page 79](#)
- [Custom Background Images, page 81](#)
- [Phone Customization Tools, page 83](#)
- [Set Up Idle Display, page 83](#)

### Custom Phone Rings

The Cisco Unified IP Phone ships with two default ring types that are implemented in hardware: Chirp1 and Chirp2. Cisco Unified Communications Manager also provides a default set of additional phone ring sounds that are implemented in software as pulse code modulation (PCM) files. The PCM files, along with an XML file (named `DistinctiveRinglist.xml`) that describes the ring list options that are available at your site, exist in the TFTP directory on each Cisco Unified Communications Manager server.

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

The following sections describe how you can customize the phone rings that are available at your site by creating PCM files and editing the `DistinctiveRinglist.xml` file.

### Set Up Custom Phone Ring

To create custom phone rings for the Cisco Unified IP Phone, perform these steps:

#### Procedure

---

- Step 1** Create a PCM file for each custom ring (one ring per file). Ensure the PCM files comply with the format guidelines that are listed in [Custom Ring File Formats, on page 80](#). 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 2** Use a text editor to edit the DistinctiveRinglist.xml file. See [Custom Ring File Formats, on page 80](#) for information about how to format this file and for a sample DistinctiveRinglist.xml file.
- Step 3** Save your modifications and close the DistinctiveRinglist.xml file.
- Step 4** To cache the new DistinctiveRinglist.xml file, stop and start the TFTP service by using Cisco Unified Serviceability or disable and reenable the “Enable Caching of Constant and Bin Files at Startup” TFTP service parameter (located in the Advanced Service Parameters).

## Custom Ring File Formats

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

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

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

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

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



### Note

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

This example shows a DistinctiveRinglist.xml file that defines two phone ring types:

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

The PCM files for the rings must meet the following requirements for proper playback on Cisco IP Phones:

- Raw PCM (no header)
- 8000 samples per second

- 8 bits per sample
- Mu-law compression
- Maximum ring size = 16080 samples
- Minimum ring size = 240 samples
- Number of samples in the ring = multiple of 240.
- Ring start and end at zero crossing.

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

## Custom Background Images

You can provide users with a choice of background images (or wallpaper) for the LCD screen on their phones. Users can select a background image by choosing **Applications > Preferences > Wallpaper** on the phone.

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



### Attention

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

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

For more information, see the “Common Phone Profile Configuration” chapter in the *Cisco Unified Communications Manager Administration Guide*.

## Set Up Custom Background Image

### Procedure

- Step 1** Create two PNG files for each image (a full-size version and a thumbnail version). Ensure the PNG files comply with the format guidelines that are listed in [Custom Background File Formats](#), on page 82.
  - Step 2** Upload the new PNG files that you created to the following subdirectory in the TFTP server for the Cisco Unified Communications Manager:  
Desktops/640x480x24
- Note** The file name and subdirectory parameters are case sensitive. Be sure to use the forward slash “/” when you specify the subdirectory path.

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

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

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

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

**Step 4** Use a text editor to edit the List.xml file. See [Custom Background File Formats, on page 82](#) for the file location, file, formatting requirements, and a sample file.

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

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

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

## Custom Background File Formats

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

Desktops/640x480x24



### Tip

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

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

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

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

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

List.xml Example



```
<CiscoIPPhoneImageList>
<ImageItem Image="TFTP:Desktops/640x480x24/TN-Fountain.png"
URL="TFTP:Desktops/640x480x24/Fountain.png"/>
<ImageItem Image="TFTP:Desktops/640x480x24/TN-FullMoon.png"
URL="TFTP:Desktops/640x480x24/FullMoon.png"/>
</CiscoIPPhoneImageList>
```

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

Each background image requires two PNG files:

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


**Tip**

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

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

- Full size image - 640 pixels (width) X 480 pixels (height).
- Thumbnail image - 123 pixels (width) X 111 pixels (height).


**Tip**

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

## Phone Customization Tools

Third-party vendors provide tools that can be used to change aspects of the phone. These tools can be used to customize ringtones and wallpaper for many of the Cisco IP Phones. For more information, see the third-party vendor documentation and <http://developer.cisco.com/>.

## Set Up Idle Display

You can specify an idle display (text only; text file size should not exceed 1M bytes) that appears on the phone screen. The idle display is an XML service that the phone invokes when the phone is idle (not in use) for a designated period and no feature menu is open.

For detailed instructions about creating and displaying the idle display, see *Creating Idle URL Graphics on Cisco IP Phone* at this URL:

[http://www.cisco.com/en/US/products/sw/voicesw/ps556/products\\_tech\\_note09186a00801c0764.shtml](http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_tech_note09186a00801c0764.shtml)

In addition, see the documentation for your particular Cisco Unified Communications Manager release for the following information:

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

### Procedure

- 
- Step 1** In Cisco Unified Communications Manager Administration, select **Device > Phone**
- Step 2** In the Idle field, enter the URL to the idle display XML Service.
- Step 3** In the Idle Timer field, enter the time that the idle phone waits before displaying the idle display XML service.
- Step 4** Select **Save**.
-



## Phone Features and Setup

---

- [Phone Features and Setup Overview, page 86](#)
- [Cisco IP Phone User Support, page 86](#)
- [Telephony Features, page 86](#)
- [Feature Support by Protocol, page 108](#)
- [Phone Button Templates, page 115](#)
- [Set Up Softkey Template, page 117](#)
- [Control Phone Web Page Access, page 120](#)
- [Calling Party Normalization, page 121](#)
- [Schedule Power Save for Cisco IP Phone, page 121](#)
- [Disable Speakerphone, page 123](#)
- [Enable Agent Greeting, page 123](#)
- [Set Up Automatic Port Synchronization, page 124](#)
- [Set Up Do Not Disturb, page 124](#)
- [Enable Device Invoked Recording, page 125](#)
- [Enable BLF for Call Lists, page 125](#)
- [Set Up Call Forward Notification, page 126](#)
- [Set Up Incoming Call Toast Timer, page 127](#)
- [Set Up Remote Port Configuration, page 127](#)
- [Set Up SSH Access, page 128](#)
- [Client Matter Codes and Forced Authorization Codes, page 128](#)
- [Set Up Phone Minimum Ring Volume, page 129](#)
- [Set Up Video Capability, page 129](#)
- [Set Up Peer Firmware Sharing, page 130](#)
- [Set Auto Save Volume, page 131](#)

## Phone Features and Setup Overview

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

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

To list supported features for all phones or for a particular phone model on your Cisco Unified Communications Manager, you can generate a Unified Communications Manager Phone Feature List report on Cisco Unified Reporting.

### Related Topics

[Cisco IP Phone User Support](#), on page 86

[International User Support](#), on page 193

[Cisco Unified Communications Manager Documentation](#), on page xiii

## Cisco IP Phone User Support

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

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

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

Consider including the following types of information on this site:

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

## Telephony Features

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

For information about using most of these features on the phone, see the *Cisco Unified IP Phone 8941 and 8945 User Guide for Cisco Unified Communications Manager (SCCP and SIP)*.

**Note**

Cisco Unified Communications Manager Administration also provides several service parameters that you can use to configure various telephony functions. For more information on accessing and configuring service parameters, see the *Cisco Unified Communications Manager Administration Guide*.

**Note**

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.

**Table 14: Telephony Features for the Cisco Unified IP Phone**

Feature	Description
Abbreviated Dialing	<p>Allows users to speed dial a phone number by entering an assigned index code (1-99) on the phone keypad.</p> <p><b>Note</b> You can use Abbreviated Dialing while on-hook or off-hook.</p> <p>Users assign index codes from the Self Care Portal.</p> <p>See:</p> <ul style="list-style-type: none"> <li>• <i>Cisco Unified Communications Manager Administration Guide</i>, “Cisco Unified IP Phone Configuration”</li> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phone”</li> </ul>
Adaptive Bandwidth Management (SIP only)	<p>Ensures that the phone correctly handles situations where there are insufficient resources for the video portion of a call. When the phone receives internal messages that indicate a lack of network resources, the phone automatically changes the video resolution.</p> <p>No configuration required.</p>
Agent Greeting	<p>Allows an agent to create and update a prerecorded greeting that plays at the beginning of a call, such as a customer call, before the agent begins the conversation with the caller. The agent can prerecord a single greeting or multiple ones as needed.</p> <p>See <a href="#">Enable Agent Greeting</a>, on page 123</p>
Any Call Pickup	<p>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.</p> <p>See the <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Call Pickup Configuration” chapter.</p>
Assisted Directed Call Park (SIP only)	<p>Lets the end user press only one button to direct-park a call. This requires you to configure a BLF Directed Call Park button. Then, when the user presses an idle BLF Directed Call Park feature button for an active call, the active call is immediately parked at the Dpark slot associated with the Directed Call Park feature button.</p> <p>See the <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Configuring Directed Call Park” section.</p>

Feature	Description
Audible Message Waiting Indicator (AMWI)	<p>A stutter tone from the handset, headset, or speakerphone indicates that a user has one or more new voice messages on a line.</p> <p><b>Note</b> The stutter tone is line-specific. The user hears it only when using the line with the waiting messages.</p> <p>See the <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phone” chapter.</p>
Audio Only Lock Icon	<p>Controls the display of the security icons on the call.</p> <p>When the Override BFCP Application Encryption Status parameter is enabled, the security icon displays based on the status of the audio call only. When the audio stream is encrypted, the Lock icon displays, even if the video stream is unencrypted.</p> <p>When the Override BFCP Application Encryption Status parameter is disabled, the Secure icon display depends on the setting of the Ignore BFCP Applications Encryption parameter. The Ignore BFCP Applications Encryption parameter controls the display of the Secure icon for the audio and video calls.</p> <p>The default for the Override BFCP Application Encryption Status parameter is Disabled.</p> <p>See the Cisco Unified Communications Manager documentation.</p>
Auto Answer	<p>Connects incoming calls automatically after a ring or two.</p> <p>Auto Answer works with either the speakerphone or the headset.</p> <p>See the <i>Cisco Unified Communications Manager Administration Guide</i>, “Directory Number Configuration” chapter.</p>
Automatic Port Synchronization	<p>When the Cisco Unified Communications Manager administrator uses the Remote Port Configuration feature to set the speed and duplex function of an IP phone remotely, loss of packets can occur if one port is slower than the other.</p> <p>See <a href="#">Set Up Automatic Port Synchronization</a>, on page 124</p>
Auto Pickup	<p>Allows a user to use one-touch pickup functionality for call pickup features.</p> <p>See the <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Call Pickup” chapter.</p>
Bandwidth Management Enhancement (SCCP only)	<p>Ensures that the phone correctly handles situations where there are insufficient resources for the video part of a call. When the phone receives internal messages that indicate a lack of resources, the phone stops sending the video part of the call. The audio part of the call continues.</p> <p>If your users complain that they cannot set up video calls, see <a href="#">Insufficient Bandwidth for Video Calls</a>, on page 178.</p> <p>No configuration required.</p>
Block external to external transfer	<p>Prevents users from transferring an external call to another external number.</p> <p>See the <i>Cisco Unified Communications Manager Features and Services Guide</i>, “External Call Transfer Restrictions” chapter.</p>

Feature	Description
Bluetooth Handsfree Profile (Cisco Unified IP Phone 8945 only)	Allows you to use Bluetooth with Cisco Unified IP Phone 8945. See the <i>Cisco Unified Communications Manager Administration Guide</i> .
Busy Lamp Field (BLF)	Allows a user to monitor the call state of a directory number associated with a speed-dial button on the phone. See the <i>Cisco Unified Communications Manager Features and Services Guide</i> , “Presence” chapter.
Busy Lamp Field (BLF) Pickup	Provides enhancements to BLF Speed Dial. Allows you to configure a Directory Number (DN) that a user can monitor for incoming calls. When the DN receives an incoming call, the system alerts the monitoring user, who can then pick up the call. See the <i>Cisco Unified Communications Manager Features and Services Guide</i> , “Call Pickup” chapter.
Call Back	Provides users with an audio and visual alert on the phone when a busy or unavailable party becomes available. See: <ul style="list-style-type: none"> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phone”</li> <li>• <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Cisco Call Back”</li> </ul>
Call Display Restrictions	Determines the information that will display for calling or connected lines, depending on the parties who are involved in the call. See: <ul style="list-style-type: none"> <li>• <i>Cisco Unified Communications Manager Administration Guide</i>, “Cisco Unified IP Phone Configuration”</li> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Understanding Route Plans”</li> <li>• <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Call Display Restrictions”</li> </ul>
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. See: <ul style="list-style-type: none"> <li>• <i>Cisco Unified Communications Manager Administration Guide</i>, “Directory Number Configuration”</li> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phone”</li> <li>• <a href="#">Customize the Self Care Portal Display</a>, on page 58</li> </ul>

Feature	Description
Call Forward All Loop Breakout	<p>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.</p> <p>See the <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phone” chapter.</p>
Call Forward All Loop Prevention	<p>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.</p> <p>See the <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phone” chapter.</p>
Call Forward Configurable Display	<p>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.</p> <p>See:</p> <ul style="list-style-type: none"> <li>• <i>Cisco Unified Communications Manager Administration Guide</i>, “Directory Number Configuration”</li> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phone”</li> </ul>
Call Forward Destination Override	<p>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.</p> <p>See the <i>Cisco Unified Communications Manager System Guide</i>, “Understanding Directory Numbers” chapter.</p>
Call Forward Notification	<p>Allows you to configure the information that the user sees when receiving a forwarded call.</p> <p>For more information, see <a href="#">Set Up Call Forward Notification</a>, on page 126.</p>
Call Log Filter Enhancement	<p>Assists the user make a call by checking the call history as the user dials and presenting a list of entries that match the digits as they are input. The user can select one of the displayed numbers instead of entering the complete telephone number.</p> <p>To disable call log filtering, the administrator enables the Simplified New Call UI field. By default, call log filtering is enabled.</p> <p>See the <i>Cisco Unified Communications Manager Administration Guide</i>.</p>
Call Park	<p>Allows users to park (temporarily store) a call and then retrieve the call by using another phone in the Cisco Unified Communications Manager system.</p> <p>See the <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Call Park and Directed Call Park” chapter.</p>



Feature	Description
Call Pickup	<p>Allows users to redirect a call that is ringing on another phone within their pickup group to their phone.</p> <p>You can configure an audio or visual alert for the primary line on the phone. This alert notifies the users that a call is ringing in their pickup group.</p> <p>See the <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Call Pickup” chapter.</p>
Call Recording	<p>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.</p> <p>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.</p> <p><b>Note</b> 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.</p> <p>See the <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Monitoring and Recording” chapter.</p>
Call Waiting	<p>Indicates (and allows users to answer) an incoming call that rings while on another call. Incoming call information appears on the phone display.</p> <p>The Cisco Unified IP Phone 8941 and 8945 supports three calls per line. Cisco Unified Communications Manager sets the Maximum Number of Calls (MNC) per line to 3 and Busy Trigger (BT) per line to 2 which is configurable. When there is no call on the line, the user can make or receive a new call. When there is one call on the line, the user can make a consultation call (Transfer or Conference) and receive another call. When there are two calls on the line, then the user can make only a consultation call.</p> <p>See <i>Cisco Unified Communications Manager System Guide</i>, “Understanding Directory Numbers” chapter.</p>
Caller ID	<p>Caller identification such as a phone number, name, or other descriptive text appear on the phone display.</p> <p>See:</p> <ul style="list-style-type: none"> <li>• <i>Cisco Unified Communications Manager Administration Guide</i>, “Cisco Unified IP Phone Configuration”</li> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Understanding Route Plans”</li> <li>• <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Call Display Restrictions”</li> <li>• <i>Cisco Unified Communications Manager Administration Guide</i>, “Directory Number Configuration”</li> </ul>

Feature	Description
Caller ID Blocking	<p>Allows a user to block their phone number or email address from phones that have caller identification enabled.</p> <p>See:</p> <ul style="list-style-type: none"> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Understanding Route Plans”</li> <li>• <i>Cisco Unified Communications Manager Administration Guide</i>, “Directory Number Configuration”</li> </ul>
Calling Party Normalization	<p>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.</p> <p>See <a href="#">Calling Party Normalization</a>, on page 121.</p>
cBarge	<p>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</p> <p>See:</p> <ul style="list-style-type: none"> <li>• <i>Cisco Unified Communications Manager Administration Guide</i>, “Cisco Unified IP Phone Configuration”</li> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phone”</li> <li>• <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Barge and Privacy”</li> </ul>
Cisco Extension Mobility	<p>Allows users to temporarily access their Cisco Unified IP Phone configuration such as line appearances, services, and speed dials from 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.</p> <p>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.</p> <p>See the “Cisco Extension Mobility” chapter in the <i>Cisco Unified Communications Manager Features and Services Guide</i>.</p>
Cisco Extension Mobility Cross Cluster (EMCC)	<p>Enables a user configured in one cluster to log into a Cisco Unified IP Phone in another cluster. Users from a home cluster log into a Cisco Unified IP Phone at a visiting cluster.</p> <p><b>Note</b> Configure Cisco Extension Mobility on Cisco Unified IP Phones before you configure EMCC.</p> <p>See the <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Cisco Extension Mobility Cross Cluster” chapter.</p>

Feature	Description
Cisco Unified Communications Manager Express (Unified CME) Version Negotiation	<p>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.</p> <p>See:</p> <ul style="list-style-type: none"> <li>• <i>Cisco Unified Communications Manager Express System Administrator Guide</i></li> <li>• <a href="#">Cisco Unified Communications Manager Express Interaction</a>, on page 15</li> </ul>
Cisco WebDialer	<p>Allows users to make calls from web and desktop applications.</p> <p>For more information, see the <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Cisco WebDialer” chapter.</p>
Classic Ringtones	<p>Supports 29 ring tones: 2 embedded in the phone firmware and 27 downloaded from the Cisco Unified Communications Manager. The feature makes the available ring tones common with other Cisco Unified IP Phones.</p> <p>No configuration required.</p>
Client Matter Codes (CMC)	<p>Enables a user to specify that a call relates to a specific client matter.</p> <p>See <a href="#">Client Matter Codes and Forced Authorization Codes</a>, on page 128.</p>
Conference	<p>Allows a user to talk simultaneously with multiple parties by calling each participant individually. Conference features include Conference and Meet Me. 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.</p> <p>See:</p> <ul style="list-style-type: none"> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Conference Bridges”</li> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phone”</li> </ul> <p><b>Note</b> Be sure to inform your users if these features are activated.</p>
Configurable Font Size	Controls the displayed font size for line labels, call session bubbles, and call history displays.
Configurable Volume Autosave	<p>Enables you to set phones to automatically save the volume level for calls or allow the users to save the volume level.</p> <p>See <a href="#">Set Auto Save Volume</a>, on page 131.</p>
CTI Applications	<p>A computer telephony integration (CTI) route point can designate a virtual device to receive multiple, simultaneous calls for application-controlled redirection.</p> <p>See the <i>Cisco Unified Communications Manager Administration Guide</i>, “CTI Route Point Configuration” chapter.</p>
Custom Background Images	<p>Provides the ability to use custom background pictures on the phone.</p> <p>See <a href="#">Custom Background Images</a>, on page 81.</p>

Feature	Description
Detect Unified CM Connection Failure	Determines the sensitivity that the phone has for detecting a connection failure to Cisco Unified Communications Manager (Unified CM). See <a href="#">Survivable Remote Site Telephony</a> , on page 51
Device Invoked Recording	Provides end users with the ability to record their telephone calls using a button. In addition, you may continue to record telephone calls using the CTI User Interface. See <a href="#">Enable Device Invoked Recording</a> , on page 125.
Direct Transfer	Allows users to connect two calls to each other (without remaining on the line). See the <i>Cisco Unified Communications Manager System Guide</i> , “Cisco Unified IP Phone” chapter.
Directed Call Park	Allows a user to transfer an active call to an available directed call park number that the user dials or speed dials. A Call Park BLF button indicates whether a directed call park number is occupied and provides speed-dial access to the directed call park number. <b>Note</b> If you implement Directed Call Park, avoid configuring the Park softkey. This prevents users from confusing the Call Park and Directed Call Park features. See the <i>Cisco Unified Communications Manager Features and Services Guide</i> , “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. See the <i>Cisco Unified Communications Manager Features and Services Guide</i> , “Call Pickup” chapter.
Distinctive Ring	Users can customize how their phone indicates an incoming call and a new voice mail message. See the <i>Cisco Unified Communications Manager Features and Services Guide</i> , “Call Pickup” chapter.
Do Not Disturb (DND)	When DND is turned on, audible or visual notifications do not occur for an incoming call. See <a href="#">Set Up Do Not Disturb</a> , on page 124.
Electronic Hookswitch	Enables users to remotely control off-hook, on-hook, and ring indication functionality from a wireless analog headset connected to the phone analog headset port. See <a href="#">Wireless Headset Using Headset Port</a> , on page 65.
Enhanced DeviceTLInfo Alarm	Provides improved CTL/ITL status to the Cisco Unified Communications Manager using the DeviceTLInfo alarm if the phone is unregistered and the CTL/ITL file is installed or updated.

Feature	Description
Enhanced Message Waiting Indicator	<p>A message on the user's screen that displays the number of new voice messages received.</p> <p>See:</p> <ul style="list-style-type: none"> <li>• <i>Cisco Unified Communications Manager Administration Guide</i>, “Message Waiting Configuration”</li> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Voice Mail Connectivity to Cisco Unified Communications Manager”</li> </ul>
E-SRST Service Improvements	<p>Enables support of video, shared line, and BLF (line status) speed dial in SRST mode.</p> <p>See <a href="#">Survivable Remote Site Telephony</a>, on page 51.</p>
Extension Mobility Size Safe and Feature Safe	<p>Allows users to temporarily access their Cisco IP Phone configuration such as line appearances, services, and speed dials from shared Cisco 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.</p> <p>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.</p> <p>For more information, go to the “Cisco Extension Mobility” chapter in the <i>Cisco Unified Communications Manager Features and Services Guide</i>.</p>
Fast Dial Service	<p>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.</p> <p>See <a href="#">Modify Phone Button Template for PAB or Fast Dial</a>, on page 117.</p>
Flexible DSCP markings	<p>Supports flexible DSCP classification for video calls. The Cisco Unified Communications Manager can apply different DSCP markings for individual calls.</p> <p>No configuration required.</p>
Forced Authorization Codes (FAC)	<p>Controls the types of calls that certain users can place.</p> <p>See <a href="#">Client Matter Codes and Forced Authorization Codes</a>, on page 128.</p>
Gateway Recording for SIP (SIP phones only)	<p>Enables the ability for phones without a Built in Bridge to record calls.</p> <p>See <i>Cisco Unified Communications Manager Features and Services Guide</i>.</p>
Group Call Pickup	<p>Allows a user to answer a call that is ringing on a directory number in another group.</p> <p>See the <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Call Pickup” chapter.</p>

Feature	Description
Headset Sidetone Control	<p>Allows an administrator to set the sidetone level of a wired headset. Available sidetone levels are:</p> <ul style="list-style-type: none"> <li>• Normal</li> <li>• Low</li> <li>• Very Low</li> <li>• Off</li> </ul> <p>See to the <i>Cisco Unified Communications Manager Administration Guide</i>, “Cisco Unified IP Phone Configuration” chapter.</p>
Hold Reversion	<p>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.</p> <p>Reverting calls are distinguished from incoming calls by a single ring or beep, depending on the new call indicator setting for the line. This notification repeats at intervals if the call is not resumed.</p> <p>A call that triggers Hold Reversion also displays an animated icon in the call bubble.</p> <p>You can configure call focus priority to favor incoming or reverting calls.</p> <p>See the <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Hold Reversion” chapter.</p>
Hold Status	<p>Enables phones with a shared line to distinguish between the local and remote lines that placed a call on hold.</p> <p>No configuration is required.</p>
Hold/Resume	<p>Allows the user to move a connected call from an active state to a held state.</p> <p>Requires no configuration, unless you want to use music on hold. See “Music on Hold” in this table for information.</p> <p>See “Hold Reversion” in this table.</p>
Hold or Resume Toggle	<p>Allows you to toggle a call between active and on-hold state.</p> <p>To place a call on hold, press Hold. To resume a call, press Hold again.</p> <p>The Hard key for this feature requires no configuration, unless you want to use music on hold. For more information, see “Hold Reversion” in this table.</p> <p>To enable a caller to hear music while on hold, see “Music on Hold” in this table.</p>
HTTP Download	<p>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.</p> <p>No configuration required.</p>
HTTPS Support	<p>Increases security by requiring communication using HTTPS.</p> <p>See the Cisco Unified Communications Manager documentation.</p>

Feature	Description
Hunt Group	<p>Provides load sharing for calls to a main directory number. A hunt group contains a series of directory numbers that can answer the incoming calls. When the first directory number in the hunt group is busy, the system hunts in a predetermined sequence for the next available directory number in the group and directs the call to that phone.</p> <p>See:</p> <ul style="list-style-type: none"> <li>• <i>Cisco Communications Manager Administration Guide</i>, “Hunt Group Configuration”</li> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Understanding Route Plans”</li> </ul>
Immediate Divert	<p>Allows a user to transfer a ringing, connected, or held call directly to a voice message system. When a call is diverted, the line becomes available to make or receive new calls.</p> <p>See the <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Immediate Divert” chapter.</p>
Incoming Call Toast Timer	<p>Allows you to set the length of time that an incoming call toast (notification) appears on the phone screen.</p> <p>See <a href="#">Set Up Incoming Call Toast Timer</a>, on page 127.</p>
Intercom	<p>Allows users to place and receive intercom calls using programmable phone buttons. You can configure intercom line buttons to:</p> <ul style="list-style-type: none"> <li>• Directly dial a specific intercom extension</li> <li>• Initiate an intercom call and then prompt the user to enter a valid intercom number</li> </ul> <p><b>Note</b> If your user logs into the same phone on a daily basis using their Cisco Extension Mobility profile, assign the phone button template that contains intercom information to their profile, and assign the phone as the default intercom device for the intercom line.</p> <p>See the <i>Cisco Unified Communications Manager Feature and Services Guide</i>, “Intercom” chapter.</p>
Join	<p>Allows users to combine two calls that are on one line to create a conference call and remain on the call.</p> <p>Some JTAPI/TAPI applications are not compatible with the Join and Direct Transfer feature implementation on the Cisco Unified IP Phone 8941 and 8945 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.</p> <p>See:</p> <ul style="list-style-type: none"> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phone” chapter</li> <li>• <i>Cisco Unified IP Phone 8941 and 8945 User Guide for Cisco Unified Communications Manager (SCCP and SIP)</i>, “Basic Call Handling” chapter, “Making Conference Calls” section</li> </ul>

Feature	Description
Join Across Lines	<p>Allows users to combine calls that are on multiple phone lines to create a conference call.</p> <p>Some JTAPI/TAPI applications are not compatible with the Join and Direct Transfer feature implementation on the Cisco Unified IP Phone 8941 and 8945 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.</p> <p>For more information, see the <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phone” chapter.</p>
Larger Font for Time/Date	<p>Enlarges the Time/Date display on the phone screen header by increasing the font size from 20 pixels to 22 pixels.</p> <p>No configuration required.</p>
Line Status for Call Lists	<p>Allows the user to see the Line Status availability status of monitored line numbers in the Call History list.</p> <p>See <a href="#">Enable BLF for Call Lists, on page 125</a>.</p>
Live Call Statistics Shortcut	<p>Enables users to view call statistics for an active call using a new shortcut on the Call Details screen.</p>
Log Out of Hunt Group	<p>Allows users to log out of a hunt group and temporarily block calls from ringing their phone when they are not available to take calls. Logging out of hunt groups does not prevent nonhunt group calls from ringing their phone.</p> <p>See:</p> <ul style="list-style-type: none"> <li>• <a href="#">Set Up Softkey Template, on page 117</a></li> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Understanding Route Plans”</li> </ul>
Malicious Caller Identification (MCID)	<p>Allows users to notify the system administrator about suspicious calls that are received.</p> <p>See:</p> <ul style="list-style-type: none"> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phone”</li> <li>• <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Malicious Call Identification”</li> </ul>
Maximum CTL File Size	<p>The maximum Certificate Trust List (CTL) file size is increased to 64KB.</p> <p>No configuration required.</p>
Meet Me Conference	<p>Allows a user to host a Meet Me conference in which other participants call a predetermined number at a scheduled time.</p> <p>See the <i>Cisco Unified Communications Manager Administration Guide</i>, “Meet-Me Number/Pattern Configuration” chapter.</p>



Feature	Description
Message Waiting	<p>Defines directory numbers for message-waiting on and message-waiting off indicator. 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.</p> <p>See:</p> <ul style="list-style-type: none"> <li>• <i>Cisco Unified Communications Manager Administration Guide</i>, “Message Waiting Configuration”</li> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Voice Mail Connectivity to Cisco Unified Communications Manager”</li> </ul>
Message Waiting Indicator	<p>A light on the handset that indicates that a user has one or more new voice messages.</p> <p>See:</p> <ul style="list-style-type: none"> <li>• <i>Cisco Unified Communications Manager Administration Guide</i>, “Message Waiting Configuration”</li> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Voice Mail Connectivity to Cisco Unified Communications Manager”</li> </ul>
Minimum Ring Volume	<p>Sets a minimum ringer volume level for an IP phone.</p> <p>The minimum ringer volume level can range from 0 to 15. The default is 0 (silent).</p> <p>See <a href="#">Set Up Phone Minimum Ring Volume</a>, on page 129.</p>
Mobile Connect	<p>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.</p> <p>See the <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Cisco Unified Mobility” chapter.</p>
Mobile Voice Access	<p>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.</p> <p>See the <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Cisco Unified Mobility” chapter.</p>

Feature	Description
Monitoring and Recording	<p>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.</p> <p>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.</p> <p><b>Note</b> 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.</p> <p>See the <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Monitoring and Recording” chapter.</p>
Multiple Calls Per Line	<p>Enables a line to support multiple calls. By default, your phone supports four active calls per line, and a maximum of 24 active calls per line. Only one call can be connected at any time; other calls are automatically placed on hold.</p> <p>The system allows you to configure the maximum calls/busy trigger to not more than 24/24 both for SCCP and SIP. The default call/busy trigger value is 4/2. This feature is supported with Cisco Unified CM 7.1(5) and later.</p> <p>See the “Directory Number Configuration” chapter in the <i>Cisco Unified Communications Manager Administration Guide</i>.</p>
Music On Hold	<p>Plays music while callers are on hold.</p> <p>See the <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Music On Hold” chapter.</p>
Mute	<p>Mutes the microphone from the handset or headset.</p> <p>No configuration required.</p>
No Alert Name	<p>Makes it easier for end users to identify transferred calls by displaying the original caller’s phone number. Transferred calls appear as an Alert Call followed by the caller’s telephone number.</p> <p>No configuration required.</p>
One Click To Home Screen	<p>Adds the ability to return to the home screen with a single button click.</p> <p>No configuration required.</p>
Onhook Pre-Dialing	<p>Allows a user to dial a number without going off hook. The user can then either pick up the handset or press Dial.</p> <p>See the <i>Cisco Unified IP Phone 8941 and 8945 User Guide for Cisco Unified Communications Manager (SCCP and SIP)</i>.</p>

Feature	Description
Other Group Pickup	<p>Allows a user to answer a call ringing on a phone in another group that is associated with the user's group.</p> <p>See the <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Call Pickup” chapter.</p>
Pause in Speed Dial	<p>Enables users to add pauses to speed-dial strings to reach destinations that require FAC, CMC, dialing pauses, and additional digits.</p> <p>See the <i>Cisco Unified IP Phone 8941 and 8945 User Guide for Cisco Unified Communications Manager (SCCP and SIP)</i>.</p>
Peer Firmware Sharing (PFS)	<p>Improves phone firmware downloads.</p> <p>See <a href="#">Set Up Peer Firmware Sharing</a>, on page 130.</p>
PLK Support for Queue Statistics	<p>Enables the users to query the call queue statistics for hunt pilots and the information appears on phone screen.</p> <p>See <a href="#">Set Up Softkey Template</a>, on page 117.</p>
Plus Dialing	<p>Allows the user to dial E.164 numbers prefixed with a plus (+) sign.</p> <p>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.</p> <p>No configuration required.</p>
Privacy	<p>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.</p> <p>See:</p> <ul style="list-style-type: none"> <li>• <i>Cisco Unified Communications Manager Administration Guide</i>, “Cisco Unified IP Phone Configuration”</li> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phone”</li> <li>• <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Barge and Privacy”</li> </ul>
Private Line Automated Ringdown (PLAR)	<p>Enables the Cisco Unified Communications Manager administrator to configure a phone number that the Cisco Unified IP Phone dials as soon as the handset goes off hook. This can be useful for phones that are designated for calling emergency or “hotline” numbers.</p> <p>See the <i>Cisco Unified Communications Manager Administration Guide</i>, “Directory Number Configuration” chapter.</p>

Feature	Description
Programmable Feature Buttons	<p>Enables you to assign features, such as New Call, Call Back, and Forward All, to line buttons.</p> <p>See:</p> <ul style="list-style-type: none"> <li>• <a href="#">Phone Button Templates, on page 115</a></li> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phone”</li> <li>• <i>Cisco Unified Communications Manager Administration Guide</i>, “Phone Button Template Configuration”</li> </ul>
Programmable Feature Buttons as Softkeys	<p>Enables you to configure features on buttons or softkeys.</p> <p>See <a href="#">Set Up Softkey Template, on page 117</a>.</p>
Quality Reporting Tool (QRT)	<p>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.</p> <p>See:</p> <ul style="list-style-type: none"> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phone”</li> <li>• <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Quality Report Tool”</li> </ul>
Redial	<p>Allows users to call the most recently dialed phone number by pressing a button or Redial.</p> <p>No configuration required.</p>
Reroute Direct Calls to Remote Destination to Enterprise Number	<p>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 the remote destination rings; the desk phone does not ring. When the call is answered on the mobile phone, the desk phone displays a <code>Remote In Use</code> message. During these calls, users can make use of various features of their mobile phone.</p> <p>See the <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Cisco Unified Mobility” chapter.</p>
Remote Port Configuration	<p>Allows you 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.</p> <p><b>Note</b> If the ports are configured for Remote Port Configuration in Cisco Unified Communications Manager; the data cannot be changed on the phone.</p> <p>See <a href="#">Set Up Remote Port Configuration, on page 127</a>.</p>
Remotely Check CTL and ITL File	<p>Enables the user to view the CTL and ITL signatures and information about the server from which the signatures were downloaded.</p> <p>See <i>Cisco Unified Communications Manager Administration Guide</i>.</p>

Feature	Description
Report CTL and ITL information	<p>Enables the phone to report the CTL and ITL information to the Cisco Unified Communications Manager so that it can be viewed in a log file.</p> <p>See <i>Cisco Unified Communications Manager Administration Guide</i>.</p>
Ring Tone Setting	<p>Identifies ring type used for a line when a phone has another active call.</p> <p>See:</p> <ul style="list-style-type: none"> <li>• <i>Cisco Unified Communications Manager Administration Guide</i>, “Directory Number Configuration”</li> <li>• <a href="#">Custom Phone Rings</a>, on page 79</li> </ul>
Ringtone and Wallpaper Customization API	<p>Allows users to customize the phone wallpaper and ringtone using third-party applications.</p> <p>See <a href="#">Phone Customization Tools</a>, on page 83.</p>
RTCP Always On	<p>Simplifies phone administration by removing the need to set the RTCP field.</p>
RTCP Control for Video	<p>You can enable the phones to transmit and receive RTCP packets for both audio and video streams in a video call.</p> <p>Configure the RTCP for video parameter from the Phone or Common Phone Profile window in the Cisco Unified Communications Manager Administration.</p> <p>See <i>Cisco Unified Communications Manager Administration Guide</i>.</p>
Secondary Load Server	<p>Enables the selection of a local server or router for phones to use, instead of the designated TFTP server.</p> <p>The server or router can be identified by a hostname or IP address. The specified server or router must be running HTTP/TFTP services and have the load file in the HTTP/TFTP path.</p> <p>See <a href="#">Set Secondary Load Server</a>, on page 40.</p>
Secure Conference	<p>Allows secure phones to place audio conference calls using a secured conference bridge.</p> <p>As new participants are added by using Confm, Join, cBarge, Barge softkeys or Meet Me conferencing, the secure call icon displays as long as all participants use secure phones.</p> <p>The Conference List displays the security level of each conference participant. Initiators can remove non-secure participants from the Conference List. Noninitiators can add or remove conference participants if the Advanced Adhoc Conference Enabled parameter is set.</p> <p>See:</p> <ul style="list-style-type: none"> <li>• <a href="#">Cisco Unified IP Phone Security</a>, on page 69</li> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Conference Bridges”</li> <li>• <i>Cisco Unified Communications Manager Administration Guide</i>, “Conference Bridge Configuration”</li> <li>• <i>Cisco Unified Communications Manager Security Guide</i></li> </ul>

Feature	Description
Secure Extension Mobility Cross Cluster	<p>Enables a user that is configured in one cluster to log in to a Cisco Unified IP Phone in another cluster. The users from a home cluster can log in to a Cisco Unified IP Phone at a visiting cluster. The visiting cluster logs in to home cluster in secure mode.</p> <p><b>Note</b> Configure Cisco Extension Mobility on Cisco Unified IP Phones before you configure EMCC.</p> <p>See <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Cisco Extension Mobility Cross Cluster” chapter.</p>
Serviceability for SIP Endpoints	<p>Enables administrators to quickly and easily gather debug information from phones.</p> <p>This feature uses SSH to remotely access each IP phone. SSH must be enabled on each phone for this feature to function.</p> <p>See <a href="#">Control Debug Information from Cisco Unified Communications Manager</a>, on page 184</p>
Services URL Button	<p>Allows users to access services from a programmable button rather than by using the Services menu on a phone.</p> <p>See:</p> <ul style="list-style-type: none"> <li>• <i>Cisco Unified Communications Manager Administration Guide</i>, “Cisco Unified IP Phone Configuration”</li> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phone Services”</li> </ul>
Services	<p>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.</p> <p>See:</p> <ul style="list-style-type: none"> <li>• <i>Cisco Unified Communications Manager Administration Guide</i>, “Cisco Unified IP Phone Configuration”</li> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phone Services”</li> </ul>
Shared Line	<p>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.</p> <p>See the <i>Cisco Unified Communications Manager System Guide</i>, “Understanding Directory Numbers” chapter.</p>
Speed Dial	<p>Dials a specified number that has been previously stored.</p> <p>See:</p> <ul style="list-style-type: none"> <li>• <i>Cisco Unified Communications Manager Administration Guide</i>, “Cisco Unified IP Phone Configuration”</li> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phone”</li> </ul>

Feature	Description
sRTP Secure Video	<p>Enables you to configure the RTCP authentication tag length for the secure video calls.</p> <p>Configure the 80-bit SRTCP field from the Phone, Common Phone Profile, or Enterprise Phone Configuration window in the Cisco Unified Communications Manager Administration.</p> <p>See the <i>Cisco Unified Communications Manager Administration Guide</i>.</p>
SSH Access	<p>Allows the administrator to enable or disable the SSH Access setting using Cisco Unified CM Administration.</p> <p>This option indicates whether the phone supports the SSH Access.</p> <p>Settings include:</p> <ul style="list-style-type: none"> <li>• Enabled: Enabling the SSH server allows the phone to accept the SSH connections.</li> <li>• Disabled (Default): Disabling the SSH server functionality of the phone blocks the SSH access to the phone.</li> </ul> <p>See <a href="#">Set Up SSH Access, on page 128</a>.</p>
Time-of-Day Routing	<p>Restricts access to specified telephony features by time period.</p> <p>See:</p> <ul style="list-style-type: none"> <li>• <i>Cisco Unified Communications Manager Administration Guide</i>, “Time Period Configuration”</li> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Time-of-Day Routing”</li> </ul>
Time Zone Update	<p>Updates the Cisco Unified IP Phone with time zone changes.</p> <p>See the <i>Cisco Unified Communications Manager Administration Guide</i>, “Date/Time Group Configuration” chapter.</p>
Transfer	<p>Allows users to redirect connected calls from their phones to another number.</p> <p>Some JTAPI/TAPI applications are not compatible with the Join and Direct Transfer feature implementation on the Cisco Unified IP Phone 8941 and 8945 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.</p>
Transfer - Direct Transfer	<p>Transfer: The first invocation of Transfer initiates a new call using the same directory number, after putting the active call on hold.</p> <p>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.</p> <p>Some JTAPI/TAPI applications are not compatible with the Join and Direct Transfer feature implementation on the Cisco Unified IP Phone 8941 and 8945 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.</p> <p>See the <i>Cisco Unified Communications Manager System Guide</i>, “Understanding Directory Numbers” chapter.</p>

Feature	Description
Unconfigured Primary Line Notification	Alerts the user when the primary line is not configured for a SIP phone, or if no line is configured for an SCCP phone. The user sees the message <i>Unprovisioned</i> on the phone screen.
User Experience Enhancements	<p>Provides the following enhancements:</p> <ul style="list-style-type: none"> <li>• When there is a voice message and a missed call, the voicemail and missed call icons display.</li> <li>• When users have a single line, they can answer an incoming call while viewing the call history.</li> </ul> <p>No configuration required.</p>
VPN Client	<p>Establishes a VPN client that is embedded in the phone, providing a simple and secure solution in situations where the phones must be located outside the trusted network or where network traffic between the phone and Cisco Unified Communications Manager must traverse untrusted networks.</p> <p>See the <i>Cisco Unified Communications Manager Security Guide</i>, “Virtual Private Network Configurations” chapter.</p>
Video Mode	<p>Allows a user to select the video display mode for viewing a video conference, depending on the modes configured in the system.</p> <p>See:</p> <ul style="list-style-type: none"> <li>• <i>Cisco Unified Communications Manager Administration Guide</i>, “Conference Bridge Configuration” chapter</li> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Understanding Video Telephony” chapter</li> </ul>
Video Mute	<p>Mutes the video from the phone screen during a video call.</p> <p>No configuration required.</p>
Video Support	<p>Enables video support on the phone.</p> <p>See:</p> <ul style="list-style-type: none"> <li>• <i>Cisco Unified Communications Manager Administration Guide</i>, “Conference Bridge Configuration” chapter</li> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Understanding Video Telephony” chapter</li> <li>• <i>Cisco VT Advantage Administration Guide</i>, “Overview of Cisco VT Advantage” chapter</li> </ul>



Feature	Description
Video Through PC	<p>Allows users to make video calls by using their Cisco Unified IP Phone, personal computer, and an external video camera.</p> <p>The feature also allows users to make video calls with Cisco Jabber or Cisco Unified Video Advantage products.</p> <p>See:</p> <ul style="list-style-type: none"> <li>• <a href="#">Set Up Video Capability, on page 129</a></li> <li>• <i>Cisco Unified Communications Manager Administration Guide</i>, “Cisco Unified IP Phone Configuration” chapter</li> </ul>
Video UI Enhancement	<p>Provides users with menu options and the Video Mute button for managing video calls.</p> <p>Users can enable or disable video transmission and enable or disable automatic video transmission.</p> <p>No configuration required.</p>
Visual Voicemail	<p>Replaces the voicemail audio prompts with a graphical interface.</p> <p>See <i>Installation and Configuration Guide for Visual Voicemail</i> located at <a href="http://www.cisco.com/en/US/partner/products/ps9829/prod_installation_guides_list.html#anchor3">http://www.cisco.com/en/US/partner/products/ps9829/prod_installation_guides_list.html#anchor3</a>.</p>
Voice Messaging System	<p>Enables callers to leave messages if calls are unanswered.</p> <p>See:</p> <ul style="list-style-type: none"> <li>• <i>Cisco Unified Communications Manager Administration Guide</i>, “Cisco Voice-Mail Port Configuration”</li> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Voice Mail Connectivity to Cisco Unified Communications Manager”</li> </ul>
W360p By Default (SIP only)	<p>Provides support for the w360p Video Resolution. During video calls, the phones negotiate the video resolution. The video window dimensions automatically adjust according to the remote video resolution.</p> <p>No configuration required.</p>
Widescreen Video Enhancement (SIP only)	<p>Provides support for the w360p Video Resolution. During video calls with a Cisco Camera, the phones negotiate the video resolution. The video window dimensions adjust according to the remote video resolution.</p> <p>No configuration required.</p>
XSI Component API Support	<p>Introduces support for RTP Streaming API and Internal URIs.</p> <p>No configuration required.</p>

## Feature Support by Protocol

This section provides information about feature support for the Cisco Unified IP Phones 8941 and 8945 using the SCCP or SIP protocol with Cisco Unified Communications Manager Release 9.0 or later.

The table provides a high-level overview of calling features and their support by protocol. This table focuses primarily on end-user calling features and is not intended to represent a comprehensive listing of all available phone features. For details about user interface differences and feature use, refer to the *Cisco Unified IP Phone 8941 and 8945 User Guide for Cisco Unified Communications Manager (SCCP and SIP)*.

The guide is available at this URL:

[http://www.cisco.com/en/US/products/ps10451/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps10451/tsd_products_support_series_home.html)

The specific sections that describe the features in the user guide are referenced in the following table.

**Table 15: Cisco Unified IP Phones 8941 and 8945 Feature Support by Protocol**

Features	Protocol: SCCP	Protocol: SIP	For more information, see the following chapter and section in the user guide
Calling Features			
Abbreviated Dialing	Supported	Supported	Calling Features, Speed Dial
Agent Greeting	Supported	Supported	Calling Features, Agent Greeting
Assisted Directed Call Park	Not supported	Supported	Calling Features, Call Park
Audible Message Waiting Indicator (AMWI)	Supported	Supported	Voice Messages, Check for voice messages
Audio Only Lock Icon	Supported	Supported	Calling features, Video Calls and Security
Auto Answer	Supported	Supported	Calling features, Auto Answer
Auto-pickup	Supported	Supported	
Automatic Port Synchronization	Supported	Supported	
Bandwidth Management Enhancement	Supported	Supported	Calling features, Video calls
Barge	Supported	Supported	Calling features, Barge
Block external to external transfer	Supported	Supported	

Features	Protocol: SCCP	Protocol: SIP	For more information, see the following chapter and section in the user guide
Bluetooth Handsfree Profile	Supported (Cisco Unified IP Phone 8945 only)	Supported (Cisco Unified IP Phone 8945 only)	
Busy Lamp Field (BLF)	Supported	Supported	Calling features, Line status
Busy Lamp Field (BLF) Pickup	Supported	Supported	Calling features, Line status
Call Back	Supported	Supported	Calling features, Call Back
Call Display Restrictions	Supported	Supported	
Call Forward All	Supported	Supported	Calling features, Call Forward
Call Forward All Breakout	Supported	Supported	
Call Forward All Loop Prevention	Supported	Supported	
Call Forward Busy	Supported	Supported	Calling features, Call Forward
Call Forward Configurable Display	Supported	Supported	
Call Forward Destination Override	Supported	Supported	
Call Forward No Answer	Supported	Supported	Calling features, Call Forward
Call Forward Notification	Supported	Supported	
Call Park	Supported	Supported	Calling features, Call Park
Call Pickup/Group Call Pickup/Directed Call Pickup	Supported	Supported	Calling features, Call Pickup

Features	Protocol: SCCP	Protocol: SIP	For more information, see the following chapter and section in the user guide
Call Recording	Supported	Supported	Calling features, Silent Monitoring and Recording
Call Waiting	Supported	Supported	Calling features, Call Waiting
Caller ID	Supported	Supported	Your Phone, Buttons and hardware
Caller ID Blocking	Supported	Supported	
Calling Party Normalization	Supported	Supported	
Cisco Extension Mobility	Supported	Supported	Calling features, Extension Mobility
Cisco Extension Mobility Cross Cluster	Supported	Supported	
Classic Ringtones	Supported	Supported	
Client Matter Code (CMC)	Supported	Supported	Calling features, Client Matter Code
Computer Telephony Integration (CTI) Applications	Supported	Some support (such as Call Park, MWI)	
Configurable Call Forward Display	Supported	Supported	
Configurable Font Size	Supported	Supported	User Preferences, Configure Displayed Font Size
Configurable Volume Autosave	Supported	Supported	
Custom Background Images	Supported	Supported	
Customization Support	Supported	Supported	
Detect Unified CM Connection Failure	Supported	Supported	

Features	Protocol: SCCP	Protocol: SIP	For more information, see the following chapter and section in the user guide
Device Invoked Recording	Supported	Supported	
Direct Transfer	Supported	Supported	
Directed Call Park	Supported	Supported	Calling features, Call Park
Do Not Disturb (DND)	Supported	Supported	Calling features, Do Not Disturb
Distinctive Ring	Supported	Supported	Phone applications, Ringtones
Electronic Hookswitch	Supported	Supported	Your phone - Wireless headsets using headset port
E-SRST Improvements	Not supported	Supported	
Enhanced Message Waiting Indicator	Not Supported	Supported	Voice messages, Voice message identification
Enhanced Version Negotiation with Unified CME	Not supported	Supported	
Extension Mobility Size Safe and Feature Safe	Supported	Supported	
Fast Dial Service	Supported	Supported	Calling features, Fast Dial
Flexible DSCP Marking	Supported	Supported	
Forced Authorization Code (FAC)	Supported	Supported	Calling features, Forced Authorization Code
Gateway Recording for SIP	Not supported	Supported	
Group Call Pickup	Supported	Supported	
Headset Sidetone Controls	Supported	Supported	
Hold	Supported	Supported	Calling features, Hold

Features	Protocol: SCCP	Protocol: SIP	For more information, see the following chapter and section in the user guide
Hold or Resume Toggle	Supported	Supported	Buttons and hardware, Hold call
Hold Reversion	Supported	Supported	Calling features, Hold Reversion
HTTP Download	Supported	Supported	
HTTPS Support	Not supported	Supported	HTTPS support
Hunt Group	Supported	Supported	Calling features, Hunt Group
iDivert	Supported	Supported	Calling features, Divert
Incoming Call Toast Timer	Supported	Supported	
Intercom	Supported	Supported	Calling features, Intercom
Join	Supported	Supported	Calling features, Join calls into conference
Join Across Lines	Supported	Supported	Calling features, Join calls into conference
Larger Font for Time/Date	Supported	Supported	
Line Status for Call Lists	Supported	Supported	
Log Out of Hunt Groups	Supported	Supported	Calling features, Sign in and out of hunt group
Malicious Call ID	Supported	Supported	Calling features, Malicious Call ID
Maximum CTL File Size	Supported	Supported	
Meet Me	Supported	Supported	Calling features, Meet Me
Message Waiting Indicator	Supported	Supported	
Minimum Ring Volume	Supported	Supported	
Mobile Connect	Supported	Supported	Calling features, Mobile Connect
Mobile Voice Access	Supported	Supported	

Features	Protocol: SCCP	Protocol: SIP	For more information, see the following chapter and section in the user guide
Multiple Calls Per Line	Supported	Supported	Calling features, Multiple Calls Per Line
Music on Hold	Supported	Supported	
Mute	Supported	Supported	Calling features, Mute
No Alert Name	Not Supported	Supported	
On-hook dialing	Supported	Supported	Calling features, On-hook dialing
One Click To Home Screen	Supported	Supported	Your Phone, Buttons and Hardware
Other Group Pickup	Supported	Supported	
Pause in Speed Dial	Not supported	Supported	
Peer Firmware Sharing	Supported	Supported	
PLK Support for Queue Statistics	Supported	Supported	Calling features, Hunt Groups
Plus Dialing	Supported	Supported	Calling features, Plus Dialing
Privacy	Supported	Supported	Calling features, Privacy
Private Line Automated Ringdown (PLAR)	Supported	Supported	
Programmable Feature Buttons	Supported	Supported	Your phone, Buttons and hardware
Programmable Feature Buttons as Softkeys	Supported	Supported	
Quality Reporting Tool (QRT)	Supported	Supported	Calling features, Quality Reporting Tool
Redial	Supported	Supported	Calling features, Redial
Remotely Check CTL and ITL file	Supported	Supported	

Features	Protocol: SCCP	Protocol: SIP	For more information, see the following chapter and section in the user guide
Report CTL and ITL information	Supported	Supported	
Ring Setting	Supported	Supported	User settings, Change ring settings per line
Ringer Volume Control	Supported	Supported	Your phone, Buttons and hardware
RTCP Always On	Supported	Supported	
RTCP control for video	Supported	Supported	
Secondary Load Server	Supported	Supported	
Secure Conference	Supported	Supported	Calling features, Conference
Serviceability for SIP Endpoints	Not supported	Supported	
Services	Supported	Supported	
Services URL button	Supported	Supported	
Shared Line	Supported	Supported	Calling features, Shared lines
sRTP Secure Video	Not supported	Supported	
Monitoring and Recording	Supported	Supported	Calling features, Silent Monitoring and Recording
Speed Dial	Supported	Supported	Calling features, Speed dial
SRST Notification	Supported	Supported	
SSH Access	Supported	Supported	
Time-of-Day Routing	Supported	Supported	
Transfer	Supported	Supported	Calling features, Transfer
Transfer - Direct Transfer	Supported	Supported	Calling features, Transfer
Time Zone Update	Supported	Supported	



Features	Protocol: SCCP	Protocol: SIP	For more information, see the following chapter and section in the user guide
User Experience Enhancements	Supported	Supported	Phone applications, Call History Voice messages, Voice message identification
Video Through PC	Supported	Supported	
Video UI Enhancement	Not supported	Supported	Phone applications, Video settings
Visual Voicemail	Supported	Supported	
Voice Mail	Supported	Supported	Voice messages
VPN Client Support	Not supported	Supported	Phone applications, VPN Client Support
W360p By Default	Not supported	Supported	
Widescreen Video Enhancement	Not supported	Supported	
XSI Component API Support	Supported	Supported	

## Phone Button Templates

Phone button templates let you assign speed dials and call-handling features to programmable line buttons. Call-handling features that can be assigned to buttons include Call Forward, Hold, and Conference.

Ideally, you modify templates before registering phones on the network. In this way, you can access customized phone button template options from Cisco Unified Communications Manager during registration.

- The default Cisco Unified IP Phone 8941 template that ships with the phone uses buttons 1 through 4 for lines.
- The default Cisco Unified IP Phone 8945 template that ships with the phone uses buttons 1 through 4 for lines.

To avoid confusion for users, do not assign a feature to a button and a softkey at the same time.

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

### Related Topics

[Set Up Softkey Template, on page 117](#)

## Modify Phone Button Template

Phone button templates let you assign speed dials and call-handling features to programmable line buttons. Call-handling features that can be assigned to buttons include Call Forward, Hold, and Conference.

### Procedure

- 
- Step 1** To modify a phone button template, in Cisco Unified Communications Manager Administration choose **Device > Device Settings > Phone Button Template**
- Step 2** To assign a phone button template to a phone, choose **Device > Phone**, and set up the Phone Button Template field.
- 

## Set Up PAB or Speed Dial as IP Phone Service

To configure PAB or Speed Dial as an IP phone service (if it is not already a service), perform these steps:

### Procedure

- 
- Step 1** From Cisco Unified Communications Manager Administration, choose **Device > Device Settings > Phone Services**.  
The Find and List IP Phone Services window displays.
- Step 2** Click **Add New**.  
The IP Phone Services Configuration window displays.
- Step 3** Enter the following settings:
- Service Name and ASCII Service Name: Enter **Personal Address Book**.
  - Service Description: Enter an optional description of the service.
  - Service URL:
    - For PAB, enter the following URL:  
**http://<Unified CM-server-name>:8080/ccmpd/login.do?name=#DEVICENAME#&service=pab**
    - For Fast Dial, enter the following URL:  
**http://<Unified-CM-server-name>:8080/ccmpd/login.do?name=#DEVICENAME#&service=fd**
  - Service Category: Select **XML Service**.
  - Service Type: Select **Directories**.
  - Enable: Select the check box.
- Step 4** Click **Save**.  
You can add, update, or delete service parameters as needed as described in the *Cisco Unified Communications Manager Administration Guide*, “Cisco Unified IP Phone Services Configuration” chapter.

**Note** If you change the service URL, remove an IP phone service parameter, or change the name of a phone service parameter for a phone service to which users are subscribed, you must click **Update Subscriptions** to update all currently subscribed users with the changes, or users must resubscribe to the service to rebuild the correct URL.

## Modify Phone Button Template for PAB or Fast Dial

You can modify a phone button template to associate a service URL with a programmable button. Doing so provides users with single-button access to the PAB and Speed Dials. Before you modify the phone button template, you must configure PAB or Speed Dials as an IP Phone service.

For more information about IP Phone services and configuring line buttons, see the documentation for your particular Cisco Unified Communications Manager release.

### Procedure

- Step 1** From Cisco Unified Communications Manager Administration, choose **Device > Device Settings > Phone Button Template**.
- Step 2** Click **Find**.
- Step 3** Select the phone model.
- Step 4** Select **Copy**, enter a name for the new template, and then select **Save**.  
The Phone Button Template Configuration window opens.
- Step 5** Identify the button that you would like to assign, and select **Service URL** from the Features drop-down list that associates with the line.
- Step 6** Select **Save** to create a new phone button template that uses the service URL.
- Step 7** Choose **Device > Phone** and open the Phone Configuration window for the phone.
- Step 8** Select the new phone button template from the Phone Button Template drop-down list.
- Step 9** Select **Save** to store the change and then select **Apply Config** to implement the change.  
The phone user can now access the Self Care Portal and associate the service with a button on the phone.

## Set Up Softkey Template

Using Cisco Unified Communications Manager Administration, you can associate up to 18 softkeys with applications that are supported by the Cisco Unified IP Phone 8941 and 8945. Cisco Unified Communications Manager support the Standard User and Standard Feature softkey template.

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.

The Cisco Unified IP Phones do not support all the softkeys that are configurable in Softkey Template Configuration on Cisco Unified Communications Manager Administration. Cisco Unified Communications Manager allows you to enable or disable some softkeys in the control policy configuration settings, but the

Cisco Unified IP Phones do not support feature control policy configuration settings. The following table lists the features, softkeys that can be configured on a softkey template, and identifies whether it is supported on the Cisco Unified IP Phones.

**Note**

Cisco Unified Communications Manager allows you to configure any softkey in a softkey template, but unsupported softkeys do not display on the phone.

**Table 16: Configurable Softkeys**

Feature	Configurable softkeys in the Softkey Template configuration	Supported as a softkey on Cisco Unified IP Phone 8941 and 8945	Notes
Answer	Answer (Answer)	Yes	—
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	—
cBarge	Conference Barge (cBarge)	Yes	Configure cBarge as a programmable line button or as a softkey.
Conference	Conference (Confrn)	Yes	Conference is a dedicated button. Only exists on video call.
Conference List	Conference List (ConfList)	Yes	Phone displays Detail.
Divert	Immediate Divert (iDivert)	Yes	Phone displays Divert.
Do Not Disturb	Toggle Do Not Disturb (DND)	Yes	Configure Do Not Disturb as a programmable line button or as a softkey.
End Call	End Call (EndCall)	Yes	Phone displays Cancel if the call is not answered.
Group Pickup	Group Pick UP (GPickUp)	Yes	—
Hold	Hold (Hold)	No	Hold is a dedicated button.

Feature	Configurable softkeys in the Softkey Template configuration	Supported as a softkey on Cisco Unified IP Phone 8941 and 8945	Notes
Hunt Group	HLog (HLog)	Yes	Configure Hunt Group as a programmable feature button.
Join	Join (Join)	No	—
Malicious Call Identification	Toggle Malicious Call Identification (MCID)	Yes	Configure Malicious Call Identification as a programmable feature button or as a softkey.
Meet Me	Meet Me (MeetMe)	Yes	—
Mobile Connect	Mobility (Mobility)	Yes	Configure Mobile Connect as a softkey.
New Call	New Call (NewCall)	Yes	Phone displays New Call.
Other Pickup	Other Pickup (oPickup)	Yes	—
PLK Support for Queue Statistics	Queue Status	Yes	—
Quality Reporting Tool	Quality Reporting Tool (QRT)	Yes	Configure Quality Reporting Tool as a programmable feature button or as a softkey.
Redial	Redial (Redial)	No	—
Remove Last Conference Participant	Remove Last Conference Participant (Remove)	Yes	Phone displays Remove when a participant is selected.
Resume	Resume (Resume)	Yes	—
Select	Select (Select)	No	—
Speed Dial	Abbreviated Dial (AbbrDial)	Yes	Phone displays SpeedDial.
Transfer	Direct Transfer (DirTrfr)	Yes	Transfer is a dedicated button.  Configure transfer (Direct Transfer policy) in the Product Specific Configuration Layout section in Phone Configuration.

Feature	Configurable softkeys in the Softkey Template configuration	Supported as a softkey on Cisco Unified IP Phone 8941 and 8945	Notes
Video Mode Command	Video Mode Command (VidMode)	No	—

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

### Procedure

- 
- Step 1** To configure softkey templates, in Cisco Unified Communications Manager Administration, select **Device > Device Settings > Softkey Template**.
- Step 2** To assign a softkey template to a phone, select **Device > Phone**, and use the Softkey Template field.
- 

## Control Phone Web Page Access

For security purposes, access to the phone web pages is disabled by default. This practice prevents access to the phone web pages and the Cisco Unified Communications Self Care Portal.



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

### Procedure

- 
- Step 1** In Cisco Unified Communications Manager Administration, choose **Device > Phone**.
- Step 2** Specify the criteria to find the phone and select **Find**, or select **Find** to display a list of all phones.
- Step 3** Select the device name to open the Phone Configuration window for the device.
- Step 4** Scroll to the Product Specific Configuration area.
- Step 5** To enable access, from the Web Access drop-down list, choose **Enabled**.
- Step 6** To disable access, from the Web Access drop-down list, choose **Disabled**.
- Step 7** Select **Save**.
-

## 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 SCCP and SIP phones support the following functions:

- For the final presentation of the calling number to the user, the phone screen displays the calling number based on the international, national, or local subscriber numbers.
  - If the call is an intracity call, the calling number presented on the phone is presented 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 phone user.

The 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.

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

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 phone screen and the globalized number in the call log directories on the phone.

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

## Schedule Power Save for Cisco IP Phone

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

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

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

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

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

## Procedure

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

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

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

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

**Table 17: PowerSave Configuration Fields**

Field	Description
Days Display Not Active	Days that the display does not turn on automatically at the time specified in the Display On Time field.  Choose the day or days from the drop-down list. To choose more than one day, Ctrl-click each day that you want.
Display On Time	Time each day that the display turns on automatically (except on the days specified in the Days Display Not Active field).  Enter the time in this field in 24-hour format, where 0:00 is midnight.  For example, to automatically turn the display on at 07:00 a.m., (0700), enter <b>07:00</b> . To turn the display on at 02:00 p.m. (1400), enter <b>14:00</b> .  If this field is blank, the display will automatically turn on at 0:00.
Display On Duration	Length of time that the display remains on after turning on at the time specified in the Display On Time field.  Enter the value in this field in the format <i>hours:minutes</i> .  For example, to keep the display on for 4 hours and 30 minutes after it turns on automatically, enter <b>04:30</b> .  If this field is blank, the phone will turn off at the end of the day (0:00).  <b>Note</b> If Display On Time is 0:00 and the display on duration is blank (or 24:00), the display will remain on continuously.



Field	Description
Display Idle Timeout	<p>Length of time that the phone is idle before the display turns off. Applies only when the display was off as scheduled and was turned on by a user (by pressing a button on the phone or lifting the handset).</p> <p>Enter the value in this field in the format <i>hours:minutes</i>.</p> <p>For example, to turn the display off when the phone is idle for 1 hour and 30 minutes after a user turns the display on, enter <b>01:30</b>.</p> <p>The default value is 01:00.</p>

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

**Step 5** Select **Apply Config**.

**Step 6** Restart the phone.

## Disable Speakerphone

By default, the speakerphone is enabled on the Cisco IP Phone.

You can disable the speakerphone by using Cisco Unified Communications Manager Administration. When the speakerphone is disabled, the Redial, New Call, and Forward All softkeys are not displayed on the phones when the user presses the speakerphone button. The softkey labels are dimmed or removed.

### Procedure

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

**Step 2** Select the phone you want to modify.

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

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

## Enable Agent Greeting

The Agent Greeting feature 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, and create and update the greetings.

When a customer calls, the agent and the caller hear the prerecorded greeting. The agent can remain on mute until the greeting ends or the agent can answer the call over the greeting.

All codecs supported for the phone are supported for Agent Greeting calls.

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

### Procedure

- 
- Step 1** From Cisco Unified Communications Manager Administration, select **Device > Phone**.
  - Step 2** Locate the IP phone that you want to configure.
  - Step 3** Scroll to the Device Information Layout pane and set **Built In Bridge** to On or Default.
  - Step 4** Select **Save**.
  - Step 5** Check the setting of the bridge:
    - a) Choose **System > Service Parameters**.
    - b) Select the appropriate Server and Service.
    - c) Scroll to the Clusterwide Parameters (Device - Phone) pane and set **Builtin Bridge Enable** to On.
    - d) Select **Save**.
- 

## Set Up Automatic Port Synchronization

You can set up synchronization on a single phone or a group of phones.

### Procedure

- 
- Step 1** To configure Automatic Port Synchronization for a single phone,
    - a) In the Cisco Unified Communications Manager Administration application, choose **Device > Phone**
    - b) Locate the phone.
    - c) In the Product Specific Configuration Layout pane, set the Automatic Port Synchronization parameter.
    - d) Select **Save**.
  - Step 2** To configure Automatic Port Synchronization for a group of phones,
    - a) In the Cisco Unified Communications Manager Administration application, choose **System > Enterprise Phone Configuration**.
    - b) Set the Automatic Port Synchronization parameter.
    - c) Select **Save**.
- 

## Set Up Do Not Disturb

When Do Not Disturb (DND) is turned on, either no audible rings occur during the ringing-in state of a call, or no audible or visual notifications of any type occur.

You can configure the phone with a phone-button template with DND as one of the selected features.

For more information, see the do not disturb information in the documentation for your particular Cisco Unified Communications Manager release.

### Procedure

- 
- Step 1** In Cisco Unified Communications Manager Administration, select **Device > Phone**.
- Step 2** Locate the phone to be configured.
- Step 3** Set the following parameters.
- Do Not Disturb: This check box allows you to enable DND on the phone.
  - DND Option: Ring Off, Call Reject, or Use Common Phone Profile Setting.
  - DND Incoming Call Alert: Choose the type of alert, if any, to play on a phone for incoming calls when DND is active.
- Note** This parameter is located on in the Common Phone Profile window and the Phone Configuration window. The Phone Configuration window value takes precedence.
- Step 4** Select **Save**.
- 

## Enable Device Invoked Recording

Configure the Device Invoked Recording feature from Cisco Unified Communications Manager Administration. For more information and detailed instructions, see the “Monitoring and Recording” chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

### Procedure

- 
- Step 1** Set the IP phone Built In Bridge to **On**.
- Step 2** Set Recording Option to **Selective Call Recording Enabled**.
- Step 3** Select the appropriate Recording Profile.
- 

## Enable BLF for Call Lists

### Procedure

- 
- Step 1** In the Cisco Unified Communications Manager Administration, select **System > Enterprise Parameters**.
- Step 2** From the BLF for Call Lists drop-down list box, choose the applicable profile.  
By default, the feature is disabled.
- Parameters that you set in the Product Specific Configuration area may also appear in the Device Configuration window for various devices and in the Enterprise Phone Configuration window. If you set these same parameters in these other windows as well, the setting that takes precedence is determined in the following order:

- 1 Device Configuration window settings
- 2 Common Phone Profile window settings
- 3 Enterprise Phone Configuration window settings

**Step 3** Select **Save**.

---

## Set Up Call Forward Notification

You can control the call forward settings.

### Procedure

---

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

**Step 2** Locate the phone to be set up.

**Step 3** Configure the Call Forward Notification fields.

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

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

---

## Set Up Incoming Call Toast Timer

You can set the time that the Incoming Call Toast (incoming call notification window) displays on the user phone.

### Procedure

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

- **Device > Phone**
- **Device > Device Settings > Common Phone Profile**
- **System > Enterprise Phone Configuration**

If you configure the parameter in multiple windows, the precedence order is:

- 1 Device > Phone**
- 2 Device > Device Settings > Common Phone Profile**
- 3 System > Enterprise Phone Configuration**

**Step 2** If required, locate the phone.

**Step 3** Set the Incoming Call Toast Timer field.

Field	Description
Incoming Call Toast Timer	<p>Gives the time, in seconds, that the toast displays. The time includes the fade-in and fade-out times for the window.</p> <p>The possible values are 3, 4, 5, 6, 7, 8, 9, 10, 15, 30, and 60.</p> <p>The default is 5.</p>

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

## Set Up Remote Port Configuration

To configure the Switch Remote Port Configuration parameter or the PC Remote Port Configuration parameter, you can configure individual phones or multiple phones.

### Procedure

**Step 1** To configure the parameter for individual phones, perform the following steps:

- a) In Cisco Unified Communications Manager Administration, choose **Device > Phone**.
- b) Select the appropriate IP phones.
- c) Scroll to the Product Specific Configuration Layout area (Switch Port Remote Configuration or PC Port Remote Configuration) and set the parameter.
- d) Select **Save**.

**Step 2** To configure the setting on multiple phones simultaneously, perform the following steps:

- a) In Cisco Unified Communications Manager Administration, choose **System > Enterprise Phone Configuration**.
  - b) Configure the Remote Port Configuration parameter.
  - c) Select **Save**.
- 

## Set Up SSH Access

You can enable or disable access to the SSH daemon through port 22. Leaving port 22 open leaves the phone vulnerable to Denial of Service (DoS) attacks. By default, the SSH daemon is disabled.

The SSH Access parameter is disabled by default. You must enable the SSH Access parameter before users of these phones can use SSH.

### Procedure

---

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

- **Device > Device Settings > Common Phone Profile**
- **Device > Phone > Phone Configuration**

**Note** If you set the parameter in both windows, the setting in the **Device > Phone > Phone Configuration** window takes precedence.

**Step 2** Select the appropriate phones.

**Step 3** Scroll to the Product Specific Configuration Layout pane and select **Enable** from the SSH Access drop-down list box.

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

---

## Client Matter Codes and Forced Authorization Codes

Client Matter Codes (CMC) and Forced Authorization Codes (FAC) enable you to manage call access and accounting.

- FAC—controls the ability for a user to dial a number.

To set up CMC or FAC, see the Cisco Unified Communications Manager documentation.

## Set Up Phone Minimum Ring Volume

The minimum ring volume is set to 0 (silent) for each phone by default.

### Procedure

- 
- Step 1** In Cisco Unified Communications Manager Administration, choose **Device > Phone**.
  - Step 2** Find a phone from the list of phones.
  - Step 3** Select **Minimum Ring Volume**.
  - Step 4** Choose a value between 0 and 15.
  - Step 5** Click **Save**.
- 

## Set Up Video Capability

The Video Through PC support feature enables the user to send or receive video on the computer when the computer is connected to a phone. For more information, see the *Cisco Unified Communications Manager Administration Guide*.




---

**Note** By default, the Video through computer option is disabled.

---

The user can enable or disable the Video through computer option in the Preferences menu. If the Video on PC option is enabled and:

- Video Capability enabled: video is received and shown on the PC display while audio remains on the phone.
- Video Capability disabled: video is not displayed either on the phone or on the PC.

The feature is dependent on SCCP or SIP protocols. IP Phones that use SIP firmware can receive video without sending video; IP phones that use SCCP firmware cannot receive and send video independently.




---

**Note** The phone must be physically connected to the first network interface card (NIC1) in the PC.

---

This feature works with products such as Cisco Jabber.

### Procedure

- 
- Step 1** In Cisco Unified Communications Manager Administration, choose **Device > Phone**.
  - Step 2** Enable the Video Capability option.
-

## Set Up Peer Firmware Sharing

When enabled, the feature allows the phone to discover like phones on the subnet that are requesting the files that make the firmware image, and to automatically assemble transfer hierarchies on a per-file basis. The individual files making up the firmware image are retrieved from the TFTP server by only the root phone in the hierarchy, and the files are then rapidly transferred down the transfer hierarchy to the other phones on the subnet that are using TCP connections.

The feature provides the following advantages in high-speed campus LAN settings:

- Limits congestion on TFTP transfers to centralized remote TFTP servers
- Eliminates the need to manually control firmware upgrades
- Reduces phone downtime during upgrades when large numbers of phones are reset simultaneously

Peer Firmware Sharing may also aid in firmware upgrades in branch or remote office deployment scenarios that run over bandwidth-limited WAN links.

This menu option indicates whether the phone supports peer firmware sharing. Settings include:

- Enabled, which is the default value.
- Disabled



### Note

Phone Firmware Release 9.1(1) and later supports HTTP and TFTP firmware download methods.

### Procedure

- Step 1** In Cisco Unified Communications Manager Administration, choose **Device > Phone**.
- Step 2** Find your phone from the list of phones that associate with the Cisco Unified Communications Manager.
- Step 3** Click on the Device Name of the phone.
- Step 4** Go to Product Specific Configuration Layout area and select **Enable** from the Peer Firmware Sharing drop-down list.  
The Peer Firmware Sharing is enabled by default.
- Step 5** Check the Override Common Settings check box for any setting in the Product Specific Configuration area that you wish to update.
  - If you do not check this check box, the corresponding parameter setting does not take effect.
  - Parameters that you set in the Product Specific Configuration area may also appear in the Phone Configuration window for various devices and in the Enterprise Phone Configuration window.

If you set these same parameters in these other windows too, the setting that takes precedence is determined in the following order:

- 1 Device Configuration window settings (highest precedence)
- 2 Common Phone Profile window settings
- 3 Enterprise Phone Configuration window settings (lowest precedence)



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

---

## Set Auto Save Volume

If you enable the feature, the phone automatically saves any volume adjustment settings so that the phone uses the same volume level for other calls.

If you disable the feature, users can use a softkey to select a specific volume level for all calls.

### Procedure

---

- Step 1** In Cisco Unified Communications Manager Administration, choose **Device > Phone**.
  - Step 2** Select a phone from the list.
  - Step 3** Select **Auto Save Volume During Call**.
  - Step 4** Select **TRUE** to enable the feature, or **FALSE** to disable the feature.
  - Step 5** Click **Save**.
-





## Corporate and Personal Directory Setup

- [Corporate Directory Setup, page 133](#)
- [Personal Directory Setup, page 133](#)
- [User Personal Directory Entries Setup, page 134](#)

### Corporate Directory Setup

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

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

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

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

### Personal Directory Setup

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

Personal Directory consists of the following features:

- Personal Address Book (PAB)
- Speed Dials
- Address Book Synchronization Tool (TABSynch)

Users can use these methods to access Personal Directory features:

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

- From the Cisco IP Phone: Choose Contacts to search the corporate directory or the user personal directory.
- From a Microsoft Windows application: Users can use the TABSync tool to synchronize their PABs with Microsoft Windows Address Book (WAB). Customers who want to use the Microsoft Outlook Address Book (OAB) should begin by importing the data from the OAB into the WAB. TabSync can then be used to synchronize the WAB with Personal Directory. For instructions about TABSync, see [Download Cisco IP Phone Address Book Synchronizer, on page 134](#) and [Set Up Synchronizer, on page 135](#).

To ensure that Cisco IP Phone Address Book Synchronizer users access only their end-user data, activate the Cisco UXL Web Service in Cisco Unified Serviceability.

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

## User Personal Directory Entries Setup

Users can configure personal directory entries on the Cisco IP Phone. To configure a personal directory, users must have access to the following:

- Self Care Portal: Make sure that users know how to access their Self Care Portal. See [Set Up User Access to the Self Care Portal, on page 57](#) for details.
- Cisco IP Phone Address Book Synchronizer: Make sure to provide users with the installer. See [Download Cisco IP Phone Address Book Synchronizer, on page 134](#).

## Download Cisco IP Phone Address Book Synchronizer

To download a copy of the synchronizer to send to your users, follow these steps:

### Procedure

- 
- Step 1** To obtain the installer, choose **Application > Plugins** from Cisco Unified Communications Manager Administration.
  - Step 2** Select **Download**, which is located next to the Cisco IP Phone Address Book Synchronizer plugin name.
  - Step 3** When the file download dialog box displays, select **Save**.
  - Step 4** Send the TabSyncInstall.exe file and the instructions in [Cisco IP Phone Address Book Synchronizer Deployment, on page 134](#) to all users who require this application.
- 

## Cisco IP Phone Address Book Synchronizer Deployment

The Cisco IP Phone Address Book Synchronizer synchronizes data that is stored in your Microsoft Windows address book with the Cisco Unified Communications Manager directory and the Self Care Portal Personal Address Book.

**Tip**

To successfully synchronize the Windows address book with the Personal Address Book, all Windows address book users should be entered in the Windows address book before you perform the following procedures.

## Install Synchronizer

To install the Cisco IP Phone Address Book Synchronizer, follow these steps:

### Procedure

- Step 1** Get the Cisco IP Phone Address Book Synchronizer installer file from your system administrator.
- Step 2** Double-click the TabSyncInstall.exe file that your administrator provided.
- Step 3** Select **Run**.
- Step 4** Select **Next**.
- Step 5** Read the license agreement information, and select the **I Accept**. Select **Next**.
- Step 6** Choose the directory in which you want to install the application and select **Next**.
- Step 7** Select **Install**.
- Step 8** Select **Finish**.
- Step 9** To complete the process, follow the steps in [Set Up Synchronizer, on page 135](#).

## Set Up Synchronizer

To configure the Cisco IP Phone Address Book Synchronizer, perform these steps:

### Procedure

- Step 1** Open the Cisco IP Phone Address Book Synchronizer.  
If you accepted the default installation directory, you can open the application by choosing **Start > All Programs > Cisco Systems > TabSync**.
- Step 2** To configure user information, select **User**.
- Step 3** Enter the Cisco IP Phone user name and password and select **OK**.
- Step 4** To configure Cisco Unified Communications Manager server information, select **Server**.
- Step 5** Enter the IP address or host name and the port number of the Cisco Unified Communications Manager server and select **OK**.  
If you do not have this information, contact your system administrator.
- Step 6** To start the directory synchronization process, select **Synchronize**.  
The Synchronization Status window provides the status of the address book synchronization. If you chose the user intervention for duplicate entries rule and you have duplicate address book entries, the Duplicate Selection window displays.

- Step 7** Choose the entry that you want to include in your Personal Address Book and select **OK**.
- Step 8** When synchronization is complete, select **Exit** to close the Cisco Unified CallManager Address Book Synchronizer.
- Step 9** To verify whether the synchronization worked, sign in to your Self Care Portal and choose **Personal Address Book**. The users from your Windows address book should be listed.
-



# PART **V**

## **Cisco Unified IP Phone Troubleshooting**

- [Monitoring Phone Systems, page 139](#)
- [Troubleshooting, page 165](#)
- [Maintenance, page 187](#)
- [International User Support, page 193](#)







## Monitoring Phone Systems

---

- [Cisco Unified IP Phone Status](#), page 139
- [Cisco IP Phone Web Page](#), page 150

### Cisco Unified IP Phone Status

This section describes how to use the following menus on the Cisco Unified IP Phone 8941 and 8945 to view model information, status messages, and network statistics for the phone:

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


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

### Display Phone Information Window

To display the Model Information screen, follow these steps.

#### Procedure

---

- Step 1** Press **Applications** .
- Step 2** Select **Phone Information**.  
If the user is connected to a secure or authenticated server, a corresponding icon (lock or certificate) displays in the Phone Information Screen to the right of the server option. If the user is not connected to a secure or authenticated server, no icon appears.
- Step 3** To exit the Model Information screen, press **Exit**.
-

## Related Topics

[Cisco IP Phone Web Page](#), on page 150

## Model Information Fields

The Model Information screen includes the options described in the table below.

**Table 18: Model Information Settings for the Cisco Unified IP Phone 8941 and 8945**

Option	Description	To change
Model Number	Model number of the phone.	Display only—cannot configure.
IP Address	IP address of the phone.	Display only—cannot configure.
Host Name	Host name of the phone.	Display only—cannot configure.
Active Load	Version of firmware currently installed on the phone.	Display only—cannot configure.
Last Upgrade	Date of the most recent firmware upgrade.	Display only—cannot configure.
Active Server	IP address or name of the server to which the phone is registered.	Display only—cannot configure.
Stand-by Server	IP address or name of the standby server.	Display only—cannot configure.

## Display Status Menu

The Status menu includes the following options, which provide information about the phone and phone operations:

- Status Messages: Displays the Status Messages screen, which shows a log of important system messages.
- Ethernet Statistic: Displays the Ethernet Statistics screen, which shows Ethernet traffic statistics.
- Call Statistics: Displays counters and statistics for the current call.

To display the Status menu, perform these steps:


### Procedure

- 
- Step 1** To display the Status menu, press **Applications**.
- Step 2** Select **Administrator Settings > Status**.
- Step 3** To exit the Status menu, press **Exit**.
-

## Display Status Messages Window

The Status Messages window displays the 30 most recent status messages that the phone has generated. You can access this screen at any time, even if the phone has not finished starting up.

### Procedure

- 
- Step 1** Press **Applications** .
  - Step 2** Select **Administrator Settings > Status > Status Messages**.
  - Step 3** To remove the current status messages, press **Clear List**.
  - Step 4** To exit the Status Messages screen, press **Exit**.
- 

### Related Topics

[Phone Displays Error Messages, on page 168](#)

[Phone Displays Error Messages, on page 168](#)

### Status Messages

The Status Messages screen displays the 10 most recent status messages that the phone has generated. You can access this screen at any time, even if the phone has not finished starting up. The following table describes the status messages that might appear. This table also includes actions you can take to address errors.

**Table 19: Status Messages on the Cisco Unified IP Phones 8941 and 8945**

Message	Description	Possible explanation and action
CFG file not found	The name-based and default configuration file was not found on the TFTP Server.	<p>The configuration file for a phone is created when the phone is added to the Cisco Unified Communications Manager database. If the phone has not been added to the Cisco Unified Communications Manager database, the TFTP server generates a CFG File Not Found response.</p> <ul style="list-style-type: none"> <li>• Phone is not registered with Cisco Unified Communications Manager. You must manually add the phone to Cisco Unified Communications Manager if you are not allowing phones to autoregister. See <a href="#">Phone Addition Methods</a>, on page 47 for details.</li> <li>• If you are using DHCP, verify that the DHCP server is pointing to the correct TFTP server.</li> <li>• If you are using static IP addresses, check configuration of the TFTP server. See <a href="#">Configure Network Settings</a>, on page 32 for details on assigning a TFTP server.</li> </ul>
CFG TFTP Size Error	The configuration file is too large for file system on the phone.	Power cycle the phone.
Checksum Error	Downloaded software file is corrupted.	Obtain a new copy of the phone firmware and place it in the TFTPPath directory. You should only copy files into this directory when the TFTP server software is shut down, otherwise the files may be corrupted.
DHCP timeout	DHCP server did not respond.	<ul style="list-style-type: none"> <li>• Network is busy: The errors should resolve themselves when the network load reduces.</li> <li>• No network connectivity between the DHCP server and the phone: Verify the network connections.</li> <li>• DHCP server is down: Check configuration of DHCP server.</li> <li>• Errors persist: Consider assigning a static IP address. See <a href="#">Configure Network Settings</a>, on page 32 for details on assigning a static IP address.</li> </ul>

Message	Description	Possible explanation and action
DNS timeout	DNS server did not respond.	<ul style="list-style-type: none"> <li>• Network is busy: The errors should resolve themselves when the network load reduces.</li> <li>• No network connectivity between the DNS server and the phone: Verify the network connections.</li> <li>• DNS server is down: Check configuration of DNS server.</li> </ul>
DNS unknown host	DNS could not resolve the name of the TFTP server or Cisco Unified Communications Manager.	<ul style="list-style-type: none"> <li>• Verify that the host names of the TFTP server or Cisco Unified Communications Manager are configured properly in DNS.</li> <li>• Consider using IP addresses rather than host names.</li> </ul>
Duplicate IP	Another device is using the IP address assigned to the phone.	<ul style="list-style-type: none"> <li>• If the phone has a static IP address, verify that you have not assigned a duplicate IP address. See <a href="#">Configure Network Settings, on page 32</a> section for details.</li> <li>• If you are using DHCP, check the DHCP server configuration.</li> </ul>
Error update locale	One or more localization files could not be found in the TFTPPath directory or were not valid. The locale was not changed.	<p>From Cisco Unified Operating System Administration, check that the following files are located within subdirectories in the TFTP File Management:</p> <ul style="list-style-type: none"> <li>• Located in subdirectory with same name as network locale: <ul style="list-style-type: none"> <li>◦ tones.xml</li> </ul> </li> <li>• Located in subdirectory with same name as user locale: <ul style="list-style-type: none"> <li>◦ glyphs.xml</li> <li>◦ dictionary.xml</li> <li>◦ kate.xml</li> </ul> </li> </ul>
File not found	The phone cannot locate, on the TFTP server, the phone load file that is specified in the phone configuration file.	From Cisco Unified Operating System Administration, make sure that the phone load file is on the TFTP server, and that the entry in the configuration file is correct.

Message	Description	Possible explanation and action
IP address released	The phone has been configured to release its IP address.	The phone remains idle until it is power cycled or you reset the DHCP address. See <a href="#">Configure Network Settings, on page 32</a> .
Load ID incorrect	Load ID of the software file is of the wrong type.	Check the load ID assigned to the phone (from Cisco Unified Communications Manager, choose <b>Device &gt; Phone</b> ). Verify that the load ID is entered correctly.
Load rejected HC	The application that was downloaded is not compatible with the phone hardware.	Occurs if you were attempting to install a version of software on this phone that did not support hardware changes on this newer phone.  Check the load ID assigned to the phone (from Cisco Unified Communications Manager, choose <b>Device &gt; Phone</b> ). Enter the load displayed on the phone.
No default router	DHCP or static configuration did not specify a default router.	<ul style="list-style-type: none"> <li>• If the phone has a static IP address, verify that the default router has been configured. See <a href="#">Configure Network Settings, on page 32</a>.</li> <li>• If you are using DHCP, the DHCP server has not provided a default router. Check the DHCP server configuration.</li> </ul>
No DNS server IP	A name was specified but DHCP or static IP configuration did not specify a DNS server address.	<ul style="list-style-type: none"> <li>• If the phone has a static IP address, verify that the DNS server has been configured. See <a href="#">Configure Network Settings, on page 32</a>.</li> <li>• If you are using DHCP, the DHCP server has not provided a DNS server. Check the DHCP server configuration.</li> </ul>
TFTP access error	TFTP server is pointing to a directory that does not exist.	<ul style="list-style-type: none"> <li>• If you are using DHCP, verify that the DHCP server is pointing to the correct TFTP server.</li> <li>• If you are using static IP addresses, check configuration of TFTP server. See <a href="#">Configure Network Settings, on page 32</a> about assigning a TFTP server.</li> </ul>

Message	Description	Possible explanation and action
TFTP file not found	The requested load file (.bin) was not found in the TFTPPath directory.	Check the load ID assigned to the phone (from Cisco Unified Communications Manager, choose <b>Device &gt; Phone</b> ). Verify that the TFTPPath directory contains a .bin file with this load ID as the name.
TFTP error	The phone does not recognize an error code provided by the TFTP server.	Contact the Cisco TAC.
TFTP server not authorized	The specified TFTP server could not be found in the phone CTL file.	<ul style="list-style-type: none"> <li>• The DHCP server has the wrong configuration file for the TFTP server. In this case, update the TFTP server configuration to specify the correct TFTP server. The CTL file was made and then the TFTP server address changed. In this case, regenerate the CTL file.</li> <li>• If the phone is using a static IP address, the phone may be configured with the wrong TFTP server address. In this case, enter the correct TFTP server address in the Network Setup menu on the phone.</li> <li>• If the TFTP server address is correct, there may be a problem with the CTL file. In this case, run the CTL client and update the CTL file, making sure that the proper TFTP servers are included in this file.</li> </ul>
TFTP timeout	TFTP server did not respond.	<ul style="list-style-type: none"> <li>• Network is busy: The errors should resolve themselves when the network load reduces.</li> <li>• No network connectivity between the TFTP server and the phone: Verify the network connections.</li> <li>• TFTP server is down: Check configuration of TFTP server.</li> </ul>
Timed Out	Supplicant attempted 802.1X transaction but timed out due to the absence of an authenticator.	Authentication typically times out if 802.1X is not configured on the switch.
Version error	The name of the phone load file is incorrect.	Make sure that the phone load file has the correct name.

Message	Description	Possible explanation and action
XmlDefault.cnf.xml, or .cnf.xml corresponding to the phone device name	Name of the configuration file.	None. This is an informational message indicating the name of the configuration file for the phone.

## Display Network Statistics Window

To display the Network Statistics window, perform these steps:

### Procedure

- 
- Step 1** Press **Applications**.
- Step 2** Select **Administrator Settings > Status > Network Statistics**.
- Step 3** To reset the Rx Frames, Tx Frames, and Rx Broadcasts statistics to 0, press **Clear**.
- Step 4** To exit the Network Statistics screen, press **Exit**.
- 

### Network Statistics Fields

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

**Table 20: Network Statistics Fields for the Cisco Unified IP Phone 8941 and 8945**

Item	Description
Tx Frames	Number of packets sent by the phone
Tx Broadcasts	Number of broadcast packets sent by the phone
Tx Unicast	Total number of unicast packets transmitted by the phone
Rx Frames	Number of packets received by the phone
Rx Broadcasts	Number of broadcast packets received by the phone
Rx Unicast	Total number of unicast packets received by the phone
Neighbor Device ID: <ul style="list-style-type: none"> <li>• Neighbor IP Address</li> <li>• Neighbor Port</li> </ul>	Identifier of a device connected to this port discovered by CDP protocol.



Item	Description
Restart Cause: One of these values: <ul style="list-style-type: none"> <li>• Hardware Reset (Power-on reset)</li> <li>• Software Reset (memory controller also reset)</li> <li>• Software Reset (memory controller not reset)</li> <li>• Watchdog Reset</li> <li>• Unknown</li> </ul>	Cause of the last reset of the phone
Port 1	Link state and connection of the PC port (for example, Auto 100 Mb Full-Duplex means that the PC port is in a link-up state and has autonegotiated a full-duplex, 100Mbps connection)
Port 2	Link state and connection of the Network port
IPv4	Information on the DHCP status. This includes the following states: CDP BOUND CDP INIT DHCP BOUND DHCP DISABLED DHCP INIT DHCP INVALID DHCP REBINDING DHCP REBOOT DHCP RENEWING DHCP REQUESTING DHCP RESYNC DHCP UNRECOGNIZED DHCP WAITING COLDBOOT TIMEOUT SET DHCP COLDBOOT SET DHCP DISABLED DISABLED DUPLICATE IP SET DHCP FAST

## Display Call Statistics Window

You can access the Call Statistics screen on the phone to display counters, statistics, and voice-quality metrics of the most recent call.



### Note

You can also remotely view the call statistics information by using a web browser to access the Streaming Statistics web page. This web page contains additional RTCP statistics that are not available on the phone. For more information about remote monitoring, see [Cisco IP Phone Web Page, on page 150](#).

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

## Procedure

- 
- Step 1** Press **Applications**.
- Step 2** Select **Administrator Settings > Status > Call Statistics**.
- Step 3** To exit the Call Statistics screen, press **Exit**.
- 

## Call Statistics Fields

The Call Statistics screen displays these items.

**Table 21: Call Statistics Fields for the Cisco Unified Phone 8941 and 8945**

Item	Description
Rcvr Codec	Type of voice stream received (RTP streaming audio from codec): G.729, G.711 u-law, G.711 A-law, G.722.
Sender Codec	Type of voice stream transmitted (RTP streaming audio from codec): G.729, G.711 u-law, G.711 A-law, G.722.
Rcvr Size	Size of voice packets, in milliseconds, in the receiving voice stream (RTP streaming audio).
Sender Size	Size of voice packets, in milliseconds, in the transmitting voice stream.
Rcvr Packets	<p>Number of RTP voice packets received since voice stream was opened.</p> <p><b>Note</b> 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.</p>

Item	Description
Sender Packets	Number of RTP voice packets transmitted since voice stream was opened. <b>Note</b> 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 in the receiving voice stream that have been discarded (bad packets, too late, and so on). <b>Note</b> The phone will discard payload type 19 comfort noise packets that are generated by Cisco Gateways, which will increment this counter.
Rcvr Lost Packets	Missing RTP packets (lost in transit).
<b>Voice Quality Metrics</b>	
Cumulative Conceal Ratio	Total number of concealment frames divided by total number of speech frames received from start of the voice stream.
Interval Conceal Ratio	Ratio of concealment frames to speech frames in preceding 3 second interval of active speech. If using voice activity detection (VAD), a longer interval might be required to accumulate 3 seconds of active speech.
Max Conceal Ratio	Highest interval concealment ratio from start of the voice stream.
Conceal Secs	Number of seconds that have concealment events (lost frames) from the start of the voice stream (includes severely concealed seconds).
Severely Conceal Secs	Number of seconds that have more than 5 percent concealment events (lost frames) from the start of the voice stream.
Latency	Estimate of the network latency, expressed in milliseconds. Represents a running average of the round-trip delay, measured when RTCP receiver report blocks are received.
MOS LQK	Objective estimate of the Mean Opinion Score (MOS) for Listening Quality (LQK) that ranks audio quality from 5 (excellent) to 1 (bad). This score is based on audible-concealment events due to a frame loss in the preceding 8 seconds of the voice stream. <b>Note</b> The MOS LQK score can vary based on the type of codec that the Cisco Unified IP Phone uses.
Avg MOS LQK	Average MOS LQK score for the entire voice stream.
Min MOS LQK	Lowest MOS LQK score from the start of the voice stream.

Item	Description
Max MOS LQK	<p>Baseline or highest MOS LQK score from the start of the voice stream.</p> <p>The following codecs provide the corresponding maximum MOS LQK scores under normal conditions with no frame loss:</p> <ul style="list-style-type: none"> <li>• G.711: 4.5</li> <li>• G.722: 4.5</li> <li>• G.728/iLBC: 3.9</li> <li>• G729A/AB: 3.7</li> </ul>
MOS LQK Version	Version of the Cisco-proprietary algorithm used to calculate the MOS LQK scores.

## Cisco IP Phone Web Page

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

- Device information: Displays device settings and related information for the phone.
- Network setup information: Displays network setup information and information about other phone settings.
- Network statistics: Displays hyperlinks that provide information about network traffic.
- Device logs: Displays hyperlinks that provide information that you can use for troubleshooting.
- Streaming statistic: Includes the Audio and Video statistics, Stream 1, Stream 2, Stream 3, Stream 4, Stream 5 and Stream 6 hyperlinks, which display a variety of streaming statistics.

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

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

### Related Topics

[Display Phone Information Window, on page 139](#)

[Control Phone Web Page Access, on page 120](#)

## Access Web Page for Phone

If you cannot access the web page, it may be disabled.

See [Control Phone Web Page Access, on page 120](#) for more information.

### Procedure

- 
- Step 1** Obtain the IP address of the Cisco Unified IP Phone using one of these methods:

- Search for the phone in Cisco Unified Communications Manager Administration by choosing **Device > Phone**. Phones registered with Cisco Unified Communications Manager display the IP address on the Find and List Phones window and at the top of the **Phone Configuration** window.
- On the Cisco Unified IP Phone, press **Applications**, choose **Administrator Settings > Network Setup**, and then scroll to the **IP Address** option.

**Step 2** Open a web browser and enter one of the following URLs, where *IP\_address* is the IP address of the Cisco Unified IP Phone:

*http://IP\_address*

or

*https://IP\_address*

## Device Information

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

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

**Table 22: Device Information Area Items**

Item	Description
MAC Address	Media Access Control (MAC) address of the phone
Host Name	Unique, fixed name that is automatically assigned to the phone based on its MAC address
Phone DN	Directory number assigned to the phone
App Load ID	Identifier of the firmware running on the phone
Boot Load ID	Identifier of the factory-installed load running on the phone
Hardware Revision	Revision value of the phone hardware
Serial Number	Unique serial number of the phone
Model Number	Model number of the phone
Message Waiting	Indicates if there is a voice message waiting on the primary line for this phone.

Item	Description
UDI	Displays the following Cisco Unique Device Identifier (UDI) information about the phone: <ul style="list-style-type: none"> <li>• Device Type: Indicates hardware type. For example, phone displays for all phone models</li> <li>• Device Description: Displays the name of the phone associated with the indicated model type</li> <li>• Product Identifier: Specifies the phone model</li> <li>• Version Identifier: Represents the hardware version of the phone</li> <li>• Serial Number: Displays the unique serial number of the phone.</li> </ul>
Time	Time obtained from the Date/Time Group in Cisco Unified Communications Manager to which the phone belongs
Time Zone	Time zone obtained from the Date/Time Group in Cisco Unified Communications Manager to which the phone belongs
Date	Date obtained from the Date/Time Group in Cisco Unified Communications Manager to which the phone belongs

## Network Setup

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

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

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

**Table 23: Network Setup Area Items**

Item	Description
DHCP Server	IP address of the Dynamic Host Configuration Protocol (DHCP) server from which the phone obtains its IP address.
MAC Address	Media Access Control (MAC) address of the phone.
Host Name	Host name that the DHCP server assigned to the phone.
Domain Name	Name of the Domain Name System (DNS) domain in which the phone resides.
IP Address	Internet Protocol (IP) address of the phone.

Item	Description
Subnet Mask	Subnet mask used by the phone.
TFTP Server 1	Primary Trivial File Transfer Protocol (TFTP) server used by the phone.
TFTP Server 2	Backup Trivial File Transfer Protocol (TFTP) server used by the phone.
Default Router	Default router used by the phone.
DNS Server	Primary Domain Name System (DNS) server (DNS Server 1) and optional backup DNS servers (DNS Server 2–5) used by the phone.
Operational VLAN ID	Auxiliary Virtual Local Area Network (VLAN) configured on a Cisco Catalyst switch in which the phone is a member.
Admin. VLAN ID	Auxiliary VLAN in which the phone is a member.
Unified CM 1 and 2	<p>Host names or IP addresses, in prioritized order, of the Cisco Unified Communications Manager servers with which the phone can register. An item can also show the IP address of an SRST router that is capable of providing limited Cisco Unified Communications Manager functionality, if such a router is available.</p> <p>For an available server, an item will show the Cisco Unified Communications Manager server IP address and one of the following states:</p> <ul style="list-style-type: none"> <li>• Active: Cisco Unified Communications Manager server from which the phone is currently receiving call-processing services.</li> <li>• Standby: Cisco Unified Communications Manager server to which the phone switches if the current server becomes unavailable.</li> <li>• Blank: No current connection to this Cisco Unified Communications Manager server.</li> </ul> <p>An item may also include the Survivable Remote Site Telephony (SRST) designation, which identifies an SRST router capable of providing Cisco Unified Communications Manager functionality with a limited feature set. This router assumes control of call processing if all other Cisco Unified Communications Manager servers become unreachable. The SRST Cisco Unified Communications Manager always appears last in the list of servers, even if it is active. You configure the SRST router address in the Device Pool section in Cisco Unified Communications Manager Configuration window.</p>
Information URL	URL of the help text that appears on the phone.
Directories URL	URL of the server from which the phone obtains directory information.
Messages URL	URL of the server from which the phone obtains message services.
Services URL	URL of the server from which the phone obtains Cisco Unified IP Phone services.

Item	Description
DHCP Enabled	Indicates whether DHCP is being used by the phone.
DHCP Address Released	Indicates the setting of the DHCP Address Released option on the phone Network Setup menu.
Alternate TFTP	Indicates whether the phone is using an alternative TFTP server.
Idle URL	URL that the phone displays when the 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 phone has not been used and no menu is open before the XML service specified by Idle URL is activated.
Proxy Server URL	URL of proxy server, which makes HTTP requests to nonlocal host addresses on behalf of the phone HTTP client and provides responses from the nonlocal host to the phone HTTP client.
Authentication URL	URL that the phone uses to validate requests made to the phone web server.
Automatic Port Synchronization	Indicates if the phone is enabled to synchronize the PC and SW ports to the same speed and to duplex mode.
SW Port Configuration	Indicates if remote port configuration of the speed and duplex mode for the switch port is enabled or disabled.
PC Port Configuration	Indicates if remote port configuration of the speed and duplex mode for the PC port is enabled or disabled.
SW Port Setup	Speed and duplex of the switch port, where: <ul style="list-style-type: none"> <li>• A: Auto Negotiate</li> <li>• 10H: 10-BaseT/half duplex</li> <li>• 10F: 10-BaseT/full duplex</li> <li>• 100H: 100-BaseT/half duplex</li> <li>• 100F: 100-BaseT/full duplex</li> <li>• 1000F: 1000-BaseT/full duplex</li> <li>• No Link: No connection to the switch port</li> </ul>



Item	Description
PC Port Setup	Speed and duplex of the PC port, where: <ul style="list-style-type: none"> <li>• A: Auto Negotiate</li> <li>• 10H: 10-BaseT/half duplex</li> <li>• 10F: 10-BaseT/full duplex</li> <li>• 100H: 100-BaseT/half duplex</li> <li>• 100F: 100-BaseT/full duplex</li> <li>• 1000F: 1000-BaseT/full duplex</li> <li>• No Link: No connection to the PC port</li> </ul>
User Locale	User locale associated with the phone user. Identifies a set of detailed information to support users, including language, font, date and time formatting, and alphanumeric keyboard text information.
Network Locale	Network locale associated with the phone user. Identifies a set of detailed information to support the phone in a specific location, including definitions of the tones and cadences used by the phone.
Headset Enabled	Indicates whether the Headset button is enabled on the phone.
User Locale Version	Version of the user locale loaded on the phone.
Network Locale Version	Version of the network locale loaded on the phone.
PC Port Disabled	Indicates whether the PC port on the phone is enabled or disabled.
Speaker Enabled	Indicates whether the speakerphone is enabled on the phone.
GARP Enabled	Indicates whether the phone learns MAC addresses from Gratuitous ARP responses.
Video Capability Enabled	Indicates whether the phone can participate in video calls when connected to an appropriately equipped PC.
Voice VLAN Enabled	Indicates whether the phone allows a device attached to the PC port to access the Voice VLAN.
DSCP for Call Control	DSCP IP classification for call control signaling.

Item	Description
DSCP for Configuration	DSCP IP classification for any phone configuration transfer.
DSCP for Services	DSCP IP classification for phone-based services.
Security Mode	Displays the security mode that is set for the phone.
Web Access Enabled	Indicates whether web access is enabled (Yes) or disabled (No) for the phone.
Span to PC Port	Indicates whether the phone will forward packets transmitted and received on the network port to the access port.
PC VLAN	VLAN used to identify and remove 802.1P/Q tags from packets sent to the PC.
LLDP-MED: Switch Port	Indicates whether Link Layer Discovery Protocol Media Endpoint Discovery (LLDP-MED) is enabled on the switch port.
LLDP Power Priority	<p>Advertises the phone's power priority to the switch, enabling the switch to appropriately provide power to the phones. Settings include:</p> <ul style="list-style-type: none"> <li>• Unknown (default)</li> <li>• Low</li> <li>• High</li> <li>• Critical</li> </ul>
LLDP Asset ID	Identifies the asset ID assigned to the phone for inventory management.
CDP: PC Port	<p>Indicates whether CDP is supported on the PC port (default is enabled).</p> <p>Enable CDP on the PC port when Cisco VT Advantage/Unified Video Advantage (CVTA) is connected to the PC port. CVTA does not work without CDP interaction with the phone.</p> <p>When CDP is disabled in Cisco Unified Communications Manager, a warning is displayed, indicating that disabling CDP on the PC port prevents CVTA from working.</p> <p>The current PC and switch port CDP values are shown on the Settings menu.</p>

Item	Description
CDP: SW Port	<p>Indicates whether CDP is supported on the switch port (default is enabled).</p> <p>Enable CDP on the switch port for VLAN assignment for the phone, power negotiation, QoS management, and 802.1x security.</p> <p>Enable CDP on the switch port when the phone is connected to a Cisco switch.</p> <p>When CDP is disabled in Cisco Unified Communications Manager, a warning is presented, indicating that CDP should be disabled on the switch port only if the phone is connected to a non-Cisco switch.</p> <p>The current PC and switch port CDP values are shown on the Settings menu.</p>

## Network Statistics

The following network statistics hyperlinks on a phone web page provide information about network traffic on the phone.

### Ethernet Information Web Page

The following table describes the items in this area.

**Table 24: Ethernet Information Items**

Item	Description
Tx Frames	Total number of packets transmitted by the phone
Tx broadcast	Total number of broadcast packets transmitted by the phone
Tx unicast	Total number of unicast packets transmitted by the phone
Rx Frames	Total number of packets received by the phone
Rx broadcast	Total number of broadcast packets received by the phone
Rx unicast	Total number of unicast packets received by the phone

### Access Area and Network Area Web Pages

The following table describes the items in this area.

**Table 25: Access Area and Network Items**

Item	Description
Tx Frames	Number of packets transmitted by the phone
Tx broadcast	Number of broadcast packets transmitted by the phone

Item	Description
Tx Unicast	Number of unicast packets transmitted by the phone
Rx Frames	Number of packets received by the phone
Rx broadcast	Number of broadcast packets received by the phone
Rx unicast	Number of unicast packets received by the phone
LLDP FramesOutTotal	Number of LLDP frames sent out from the phone
LLDP AgeoutsTotal	Number of LLDP frames that have been time out in cache
LLDP FramesDiscardedTotal	Number of LLDP frames that are discarded when any of the mandatory TLVs is missing or out of order or contains out of range string length.
LLDP FramesInErrorsTotal	Number of LLDP frames that received with one or more detectable errors.
LLDP FramesInTotal	Number of LLDP frames received on the phone.
LLDP TLVDiscardedTotal	Number of LLDP TLVs that are discarded.
LLDP TLVUnrecognizedTotal	Number of LLDP TLVs that are not recognized on the phone.
CDP Neighbor Device ID	Identifier of a device connected to this port discovered by CDP protocol.
CDP Neighbor IP Address	IP address of the neighbor device discovered by CDP protocol.
CDP Neighbor Port	Neighbor device port to which the phone is connected discovered by CDP protocol.
LLDP Neighbor Device ID	Identifier of a device connected to this port discovered by LLDP protocol.
LLDP Neighbor IP Address	IP address of the neighbor device discovered by LLDP protocol.
LLDP Neighbor Port	Neighbor device port to which the phone is connected discovered by LLDP protocol.
Port Information	Speed and duplex information.
IPv4	Information on the DHCP status.

## Device Logs

The following device logs hyperlinks on a phone web page provide information you can use to help monitor and troubleshoot the phone. To access a device log area, access the web page for the phone as described in [Access Web Page for Phone](#), on page 150.

- **Console Logs:** Includes hyperlinks to individual log files. The console log files include debug and error messages received on the phone.
- **Core Dumps:** Includes hyperlinks to individual dump files. The core dump files include data from a phone crash.
- **Status Messages:** Displays up to the 10 most recent status messages that the phone has generated since it was last powered up. You can also see this information from the Status Messages screen on the phone. [Status Messages, on page 141](#) describes the status messages that can appear.
- **Debug Display:** Displays debug messages that might be useful to Cisco TAC if you require assistance with troubleshooting.
- **Restart Cause:** Displays the cause for the restart.

## Streaming Statistics

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

The streaming statistics areas on a phone web page provide information about the streams. Cisco Unified IP Phone 8941 and 8945 use only Stream 1.

To display a Streaming Statistics area, access the web page for the phone, and then click the Stream 1 hyperlink. The following table describes the fields in the Streaming Statistics areas.

**Table 26: Streaming Statistics Fields**

Item	Description
Remote Address	IP address and RTP port of the destination of the stream.
Local Address	IP address and RTP port of the phone.
Start Time	Internal time stamp indicating when Cisco Unified Communications Manager requested that the phone start transmitting packets.
Stream Status	Indication of whether streaming is active or not.
Host Name	Unique, fixed name that is automatically assigned to the phone based on its MAC address.
Sender Packets	Total number of RTP data packets transmitted by the phone since starting this connection. The value is 0 if the connection is set to receive only mode.
Sender Octets	Total number of payload octets transmitted in RTP data packets by the phone since starting this connection. The value is 0 if the connection is set to receive only mode.
Sender Codec	Type of audio/video encoding used for the transmitted stream.
Sender Reports Sent (see note)	Number of times the RTCP Sender Report have been sent.

Item	Description
Sender Report Time Sent (see note)	Internal time stamp indication when the last RTCP Sender Report was sent.
Rcvr Lost Packets	Total number of RTP data packets that have been lost since starting receiving data on this connection. Defined as the number of expected packets less the number of packets actually received, where the number of received packets includes any that are late or duplicate. The value displays as 0 if the connection was set to send-only mode.
Avg Jitter	Estimate of mean deviation of the RTP data packet inter-arrival time, measured in milliseconds. The value displays as 0 if the connection was set to send-only mode.
Rcvr Codec	Type of audio/video encoding used for the received stream.
Rcvr Reports Sent (see note)	Number of times the RTCP Receiver Reports have been sent.
Rcvr Report Time Sent (see note)	Internal time stamp indication when a RTCP Receiver Report was sent.
Rcvr Packets	Total number of RTP data packets received by the phone since starting receiving data on this connection. Includes packets received from different sources if this is a multicast call. The value displays as 0 if the connection was set to send-only mode.
Rcvr Octets	Total number of payload octets received in RTP data packets by the device since starting reception on the connection. Includes packets received from different sources if this is a multicast call. The value displays as 0 if the connection was set to send-only mode.
MOS LQK	Objective estimate of the Mean Opinion Score (MOS) for Listening Quality (LQK) that ranks audio quality from 5 (excellent) to 1 (bad). This score is based on audible-concealment events due to a frame loss in the preceding 8 seconds of the voice stream.  <b>Note</b> The MOS LQK score can vary based on the type of codec that the Cisco Unified IP Phone uses.
Avg MOS LQK	Average MOS LQK score for the entire voice stream.
Min MOS LQK	Lowest MOS LQK score from the start of the voice stream.

Item	Description
Max MOS LQK	<p>Baseline or highest MOS LQK score from the start of the voice stream.</p> <p>The following codecs provide the corresponding maximum MOS LQK scores under normal conditions with no frame loss:</p> <ul style="list-style-type: none"> <li>• G.711: 4.5</li> <li>• G.722: 4.5</li> <li>• G.728/iLBC: 3.9</li> <li>• G729A/AB: 3.7</li> </ul>
MOS LQK Version	Version of the Cisco-proprietary algorithm used to calculate the MOS LQK scores.
Cumulative Conceal Ratio	Total number of concealment frames divided by total number of speech frames received from start of the voice stream.
Interval Conceal Ratio	Ratio of concealment frames to speech frames in preceding 3-second interval of active speech. If using voice activity detection (VAD), a longer interval might be required to accumulate 3 seconds of active speech.
Max Conceal Ratio	Highest interval concealment ratio from start of the voice stream.
Conceal Secs	Number of seconds that have concealment events (lost frames) from the start of the voice stream (includes severely concealed seconds).
Severely Conceal Secs	Number of seconds that have more than 5 percent concealment events (lost frames) from the start of the voice stream.
Latency (see note)	Estimate of the network latency, expressed in milliseconds. Represents a running average of the round-trip delay, measured when RTCP receiver report blocks are received.
Max Jitter	Maximum value of instantaneous jitter, in milliseconds.
Sender Size	RTP packet size, in milliseconds, for the transmitted stream.
Sender Reports Received (see note)	Number of times RTCP Sender Reports have been received.
Sender Report Time Received (see note)	Last time at which an RTCP Sender Report was received.
Rcvr Size	RTP packet size, in milliseconds, for the received stream.
Rcvr Discarded	RTP packets received from network but discarded from jitter buffers.
Rcvr Reports Received (see note)	Number of times RTCP Receiver Reports have been received.

Item	Description
Rcvr Report Time Received (see note)	Last time at which an RTCP Receiver Report was received.
Sender Frames	Number of video frames transmitted by the camera/phone since the video stream was opened.
Sender Partial Frames	Number of P-frames sent by the camera, since the video stream was opened.
Sender IFrames	Number of I-frames sent by the camera, since the video stream was opened.
Sender Frame Rate	Rate at which video frames are transmitted. (Frames per second).
Sender Bandwidth	Bandwidth of the video steam that is being transmitted, in kbps (kilo bits per second).
Sender Resolution	Resolution of the video stream transmitted by the camera. For example, VGA(640x480), CIF (352x288), QCIF (176x144).
Rcvr Frames	Number of video frames received by the phone since the video stream was opened.
Rcvr Partial Frames	Number of P-frames received by the camera, since the video stream was opened.
Rcvr IFrames	Number of I-frames received by the camera, since the video stream was opened.
Rcvr IFrames Req	Number of times IDR requests sent by the phone to the remote end point, since the video stream was opened.
Rcvr Frame Rate	Rate at which video frames are received. (Frames per second).
Rcvr Frames Lost	Total number of packets lost.
Rcvr Frame Errors	Number of errors reported by video decoder, since the video stream was opened.
Rcvr Bandwidth	Bandwidth of the video steam that is being received, in kbps (kilo bits per second).
Rcvr Resolution	Resolution of the video stream received by the phone from the remote end point. For example, VGA(640x480), CIF (352x288), QCIF (176x144).
Domain	Domain of the phone.
Sender Joins	Number of times the phone has started transmitting a stream.
Rcvr Joins	Number of times the phone has started receiving a stream.



Item	Description
Bytes	Number of times the phone has stopped transmitting a stream.
Sender Start Time	Timestamp indicating when the first RTP packet is sent to the network.
Rcvr Start Time	Timestamp indicating when the first RTP packet is received from the network.

**Note**

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





## Troubleshooting

- [General Troubleshooting Information, page 165](#)
- [Startup Problems, page 167](#)
- [Phone Reset Problems, page 171](#)
- [Cisco IP Phone Security Problems, page 173](#)
- [Audio and Video Problems , page 177](#)
- [General Telephone Call Problems, page 179](#)
- [Troubleshooting Procedures, page 180](#)

### General Troubleshooting Information

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

**Table 27: Cisco Unified IP Phone General Troubleshooting**

Summary	Explanation
Connecting a Cisco Unified IP Phone to another Cisco Unified IP Phone.	Cisco does not support connecting an IP phone to another IP phone through the PC port. Each IP phone should directly connect to a switch port. If phones are connected together in a line (by using the PC port), the phones will not work.
Prolonged broadcast storms cause IP phones to reset, or be unable to make or answer a call.	A prolonged Layer 2 broadcast storm (lasting several minutes) on the voice VLAN may cause IP phones to reset, lose an active call, or be unable to initiate or answer a call. Phones may not come up until a broadcast storm ends.

Summary	Explanation
Moving a network connection from the phone to a workstation.	<p>If you are powering your phone through the network connection, you must be careful if you decide to unplug the phone network connection and plug the cable into a desktop computer.</p> <p><b>Caution</b> The network card of the computer cannot receive power through the network connection; if power comes through the connection, the network card can be destroyed. To protect a network card, wait 10 seconds or longer after unplugging the cable from the phone before plugging it into a computer. This delay gives the switch enough time to recognize that there is no longer a phone on the line and to stop providing power to the cable.</p>
Changing the telephone configuration.	By default, the network setup options are locked to prevent users from making changes that could impact their network connectivity. You must unlock the network setup options before you can configure them.
Phone resetting.	The phone resets when it loses contact with the Cisco Unified Communications Manager software. This lost connection can be due to any network connectivity disruption, including cable breaks, switch outages, and switch reboots.
Codec mismatch between the phone and another device.	The RxType and the TxType statistics show the codec that is being used for a conversation between this Cisco Unified IP phone and the other device. The values of these statistics should match. If they do not, verify that the other device can handle the codec conversation, or that a transcoder is in place to handle the service.
Sound sample mismatch between the 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 Cisco Unified IP phone and the other device. The values of these statistics should match.
Loopback condition.	<p>A loopback condition can occur when the following conditions are met:</p> <ul style="list-style-type: none"> <li>• The SW Port Configuration option in the Network Setup menu on the phone is set to <b>10 Half</b> (10-BaseT / half duplex)</li> <li>• The phone receives power from an external power supply</li> <li>• The phone is powered down (the power supply is disconnected)</li> </ul> <p>In this case, the switch port on the phone can become disabled and the following message will appear in the switch console log:</p> <pre>HALF_DUX_COLLISION_EXCEED_THRESHOLD</pre> <p>To resolve this problem, enable the port from the switch.</p>

### Related Topics

[Apply a Phone Password, on page 31](#)

[Display Call Statistics Window, on page 148](#)

## Startup Problems

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

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

### Related Topics

[Phone Startup Process](#), on page 40

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

### Problem

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

### Cause

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

### Solution

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

- Verify that the network port is functional:
  - Exchange the Ethernet cables with cables that you know are functional.
  - Disconnect a functioning Cisco IP Phone from another port and connect it to this network port to verify that the port is active.
  - Connect the Cisco IP Phone that does not start up to a different network port that is known to be good.
  - Connect the Cisco IP Phone that does not start up directly to the port on the switch, eliminating the patch panel connection in the office.
- Verify that the phone is receiving power:
  - If you are using external power, verify that the electrical outlet is functional.
  - If you are using in-line power, use the external power supply instead.
  - If you are using the external power supply, switch with a unit that you know to be functional.
- If the phone still does not start up properly, power up the phone with the handset off-hook. When the phone is powered up in this way, it attempts to launch a backup software image.
- If the phone still does not start up properly, perform a factory reset of the phone.

- After you attempt these solutions, if the phone screen on the Cisco IP Phone does not display any characters after at least five minutes, contact a Cisco technical support representative for additional assistance.

**Related Topics**

[Phone Startup Process, on page 40](#)

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

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

In addition, problems with security may prevent the phone from starting up properly. See [Troubleshooting Procedures, on page 180](#) for more information.

### Phone Displays Error Messages

**Problem**

Status messages display errors during startup.

**Solution**

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

**Related Topics**

[Display Status Messages Window, on page 141](#)

[Display Status Messages Window, on page 141](#)

### Phone Displays Message: Unprovisioned

**Problem**

The phone displays Unprovisioned on the LCD.

**Cause**

The primary line is not configured.

**Solution**

Configure the primary line.

**Related Topics**

[Set Up Cisco Unified IP Phone, on page 44](#)

## Phone Cannot Connect to TFTP Server or to Cisco Unified Communications Manager

### Problem

If the network is down between the phone and either the TFTP server or Cisco Unified Communications Manager, the phone cannot start up properly.

### Solution

Ensure that the network is currently running.

## Phone Cannot Connect to TFTP Server

### Problem

The TFTP server settings may not be correct.

### Solution

Check the TFTP settings.

### Related Topics

[Check TFTP Settings, on page 181](#)

## Phone Cannot Connect to Server

### Problem

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

### Solution

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

### Related Topics

[Check DHCP Settings, on page 181](#)

## Phone Cannot Connect Using DNS

### Problem

The DNS settings may be incorrect.

### Solution

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

### Related Topics

[Verify DNS Settings, on page 182](#)

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

### Problem

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

### Solution

If the Cisco Unified Communications Manager service is not running, all devices on the network that rely on it to make phone calls are affected. If the TFTP service is not running, many devices cannot start up successfully. For more information, see [Start Service, on page 184](#).

## Configuration File Corruption

### Problem

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

### Solution

Create a new phone configuration file.

## Cisco Unified Communications Manager Phone Registration

### Problem

The phone is not registered with the Cisco Unified Communications Manager

### Solution

A Cisco IP Phone can register with a Cisco Unified Communications Manager server only if the phone is added to the server or if autoregistration is enabled. Review the information and procedures in [Phone Addition Methods, on page 47](#) to ensure that the phone is added to the Cisco Unified Communications Manager database.

To verify that the phone is in the Cisco Unified Communications Manager database, choose **Device > Phone** from Cisco Unified Communications Manager Administration. Click **Find** to search for the phone based on the MAC Address. For information about determining a MAC address, see [Determine the Phone MAC Address, on page 43](#).

If the phone is already in the Cisco Unified Communications Manager database, the configuration file may be damaged. See [Configuration File Corruption, on page 170](#) for assistance.



## Cisco IP Phone Cannot Obtain IP Address

### Problem

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

### Solution

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

## Phone Reset Problems

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

Typically, a phone resets if it has problems in connecting to the network or to Cisco Unified Communications Manager.

## Phone Cannot Connect to LAN

### Problem

The physical connection to the LAN may be broken.

### Solution

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

## Phone Resets Due to Intermittent Network Outages

### Problem

Your network may be experiencing intermittent outages.

### Solution

Intermittent network outages affect data and voice traffic differently. Your network might be experiencing intermittent outages without detection. If so, data traffic can resend lost packets and verify that packets are received and transmitted. However, voice traffic cannot recapture lost packets. Rather than retransmitting a lost network connection, the phone resets and attempts to reconnect to the network. Contact the system administrator for information on known problems in the voice network.

## Phone Resets Due to DHCP Setting Errors

### Problem

The DHCP settings may be incorrect.

### Solution

Verify that you have properly configured the phone to use DHCP. Verify that the DHCP server is set up properly. Verify the DHCP lease duration. We recommend that you set the lease duration to 8 days.

### Related Topics

[Check DHCP Settings, on page 181](#)

## Phone Resets Due to Incorrect Static IP Address

### Problem

The static IP address assigned to the phone may be incorrect.

### Solution

If the phone is assigned a static IP address, verify that you have entered the correct settings.

## Phone Resets During Heavy Network Usage

### Problem

If the phone appears to reset during heavy network usage, it is likely that you do not have a voice VLAN configured.

### Solution

Isolating the phones on a separate auxiliary VLAN increases the quality of the voice traffic.

## Phone Resets Due to Intentional Reset

### Problem

If you are not the only administrator with access to Cisco Unified Communications Manager, you should verify that no one else has intentionally reset the phones.

### Solution

You can check if a Cisco Unified IP Phone received a command from Cisco Unified Communications Manager to reset by pressing **Applications** on the phone and choosing **Administrator Settings > Status > Network Statistics**.

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

## Phone Resets Due to DNS or Other Connectivity Issues

### Problem

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

### Solution

If the phone continues to reset, eliminate DNS or other connectivity errors by following the procedure in [Determine DNS or Connectivity Issues](#), on page 183.

## Phone Does Not Power Up

### Problem

The phone does not appear to be powered up.

### Solution

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

# Cisco IP Phone Security Problems

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

## CTL File Problems

The following sections describe troubleshooting problems with the CTL file.

### Authentication Error, Phone Cannot Authenticate CTL File

#### Problem

A device authentication error occurs.

#### Cause

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

**Solution**

Install a correct certificate.

**Phone Cannot Authenticate CTL File****Problem**

Phone cannot authenticate the CTL file.

**Cause**

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

**Solution**

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

**CTL File Authenticates but Other Configuration Files Do Not Authenticate****Problem**

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

**Cause**

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

**Solution**

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

**Phone Does Not Register****Problem**

Phone does not register with Cisco Unified Communications Manager.

**Cause**

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

**Solution**

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

**Signed Configuration Files Are Not Requested****Problem**

Phone does not request signed configuration files.

**Cause**

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

**Solution**

Configure TFTP entries with certificates in the CTL file.

## 802.1X Authentication Problems

802.1X authentication problems can be broken into the categories that are described in the following table.

**Table 28: 802.1X Authentication Problem Identification**

If all the following conditions apply,	See
<ul style="list-style-type: none"> <li>• Phone cannot obtain a DHCP-assigned IP address.</li> <li>• Phone does not register with Cisco Unified Communications Manager.</li> <li>• Phone status displays <i>Configuring IP</i> or <i>Registering</i>.</li> <li>• 802.1X Authentication Status displays <i>Held</i>.</li> <li>• Status menu 802.1X status displays <i>Failed</i>.</li> </ul>	<a href="#">802.1X Enabled on Phone but Phone Does Not Authenticate, on page 176</a>
<ul style="list-style-type: none"> <li>• Phone cannot obtain a DHCP-assigned IP address.</li> <li>• Phone does not register with Cisco Unified Communications Manager.</li> <li>• Phone status displays <i>Configuring IP</i> or <i>Registering</i>.</li> <li>• 802.1X Authentication Status displays <i>Disabled</i>.</li> <li>• Status menu displays that the DHCP status has timed out.</li> </ul>	<a href="#">802.1X Not Enabled, on page 176</a>

If all the following conditions apply,	See
<ul style="list-style-type: none"> <li>• Phone cannot obtain a DHCP-assigned IP address.</li> <li>• Phone does not register with Cisco Unified Communications Manager.</li> <li>• Phone status display as Configuring IP or Registering.</li> <li>• You are unable to access phone menus to verify 802.1X status.</li> </ul>	<a href="#">Factory Reset of Phone Has Deleted 802.1X Shared Secret, on page 176</a>

## 802.1X Enabled on Phone but Phone Does Not Authenticate

### Problem

The phone cannot authenticate.

### Cause

These errors typically indicate that 802.1X authentication is enabled on the phone, but the phone is unable to authenticate.

### Solution

To resolve this problem, check the 802.1X and shared secret configuration. See [Identify 802.1X Authentication Problems, on page 183](#).

## 802.1X Not Enabled

### Problem

The phone does not have 802.1X configured.

### Cause

These errors typically indicate that 802.1X authentication is not enabled on the phone.

### Solution

If 802.1X is not enabled on the phone, see 802.1X Authentication section.

## Factory Reset of Phone Has Deleted 802.1X Shared Secret

### Problem

After a reset, the phone does not authenticate.

**Cause**

These errors typically indicate that the phone has completed a factory reset while 802.1X was enabled. A factory reset deletes the shared secret, which is required for 802.1X authentication and network access.

**Solution**

To resolve this situation, temporarily move the phone to a network environment that is not using 802.1X authentication. After the phone starts up normally, access the 802.1X configuration menus to enable device authentication and to reenter the shared secret. See 802.1X Authentication section for details.

**Related Topics**

[Basic Reset, on page 187](#)

## Audio and Video Problems

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

### Phone Display Is Wavy

**Problem**

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

**Cause**

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

**Solution**

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

### No Speech Path

**Problem**

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

**Solution**

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

### Choppy Speech

**Problem**

A user complains of choppy speech on a call.

**Cause**

There may be a mismatch in the jitter configuration.

**Solution**

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

## Poor Audio Quality with Calls that Route Outside Cisco Unified Communications Manager

**Problem**

Poor quality occurs with tandem audio encoding. Tandem encoding can occur when calls are made between an IP Phone and a digital cellular phone, when a conference bridge is used, or in situations where IP-to-IP calls are partially routed across the PSTN.

**Cause**

In these cases, use of voice codecs such as G.729 and iLBC may result in poor voice quality.

**Solution**

Use the G.729 and iLBC codecs only when absolutely necessary.

## Insufficient Bandwidth for Video Calls

**Problem**

Users report that calls with video suddenly drop the video component of the call. The video part of a call cannot be established.

**Cause**

The network has run out of resources for the video call.

**Solution**

Changes need to be made on the Cisco Unified Communications Manager. For more information, see *Cisco Unified Communications Manager Systems Guide*.

## Video Changes Resolution

**Problem**

Users report that calls with video change the video resolution (become more grainy) during the call.

**Cause**

The network is experiencing network resource limitations and the phone is attempting to compensate by changing the video resolution.



**Solution**

Changes need to be made on the Cisco Unified Communications Manager. For more information, see the *Cisco Unified Communications Manager Systems Guide*.

## General Telephone Call Problems

The following sections help troubleshoot general telephone call problems.

### VPN-Connected Phone Does Not Log Calls

**Problem**

A remote location (home office) phone that is connected through the VPN does not log missed, placed, or received calls.

**Cause**

Without explicitly setting the Alternate TFTP setting, the Cisco IP Phone cannot contact the TFTP server and download the configuration and other files, and function properly.

**Solution**

Set up the phone to use the Alternate TFTP server and configure the TFTP server IP address.

**Related Topics**

[Set Up Remote Phone](#), on page 180

### Phone Call Cannot Be Established

**Problem**

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

**Cause**

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

**Solution**

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

## Phone Does Not Recognize DTMF Digits or Digits Are Delayed

### Problem

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

### Cause

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

### Solution

Keys should not be pressed rapidly.

## Troubleshooting Procedures

These procedures can be used to identify and correct problems.

### Set Up Remote Phone

Cisco IP Phones that are configured for SSL VPN to ASA using the built-in client in a remote location (for example, a home office) have a special configuration requirement.

We recommend that you provide the phone with an Alternate TFTP server setting manually. This setting allows the phone to download the configuration and other files from TFTP. The phone in a remote location (home office) cannot correctly provide OPTION 150 to the phone using DHCP.

The IP phone can register to the last-known Cisco Unified Communications Manager, but any configuration updates cannot be applied until you configure the manual TFTP server address.

### Procedure

---

- Step 1** On the phone, select **Applications**.
  - Step 2** Navigate to the **IPv4 Settings** window.
  - Step 3** Scroll to the Alternate TFTP option and set the field to **Yes**.
  - Step 4** In the TFTP Server 1 field, set the TFTP server address.
  - Step 5** Save the changes.
- 

### Related Topics

[Install Cisco Unified IP Phone, on page 29](#)

## Check TFTP Settings

### Procedure

- 
- Step 1** You can determine the IP address of the TFTP server that the phone uses by pressing **Applications**, then selecting **Administrator Settings > Network Setup > IPv4 Setup > TFTP Server 1**.
- Step 2** If you have assigned a static IP address to the phone, you must manually enter a setting for the TFTP Server 1 option.
- Step 3** If you are using DHCP, the phone obtains the address for the TFTP server from the DHCP server. Check that the IP address is configured in Option 150.
- Step 4** You can also enable the phone to use an alternate TFTP server. Such a setting is particularly useful if the phone recently moved from one location to another.
- Step 5** If the local DHCP does not offer the correct TFTP address, enable the phone to use an alternate TFTP server. This is often necessary in VPN scenario.
- 

### Related Topics

[Phone Cannot Connect to TFTP Server](#), on page 169

## Check DHCP Settings

### Procedure

- 
- Step 1** On the Cisco Unified IP Phone, press **Applications**.
- Step 2** Select **Administrator Settings > Network Setup > IPv4 Setup**, and look at the following options:
- **DHCP Server:** If you have assigned a static IP address to the phone, you do not need to enter a value for the DHCP Server option. However, if you are using a DHCP server, this option must have a value. If no value is found, check your IP routing and VLAN configuration. See the *Troubleshooting Switch Port and Interface Problems* document, available at this URL:  
[http://www.cisco.com/en/US/customer/products/hw/switches/ps708/prod\\_tech\\_notes\\_list.html](http://www.cisco.com/en/US/customer/products/hw/switches/ps708/prod_tech_notes_list.html)
  - **IP Address, Subnet Mask, Default Router:** If you have assigned a static IP address to the phone, you must manually enter settings for these options.
- Step 3** If you are using DHCP, check the IP addresses that your DHCP server distributes. See the *Understanding and Troubleshooting DHCP in Catalyst Switch or Enterprise Networks* document, available at this URL:  
[http://www.cisco.com/en/US/tech/tk648/tk361/technologies\\_tech\\_note09186a00800f0804.shtml](http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a00800f0804.shtml)
-

### Related Topics

[Phone Cannot Connect to Server, on page 169](#)

[Phone Resets Due to DHCP Setting Errors, on page 172](#)

## Verify DNS Settings

To verify DNS settings, follow these steps:

### Procedure

- 
- Step 1** Press **Applications**.
  - Step 2** Select **Administrator Settings > Network Setup > IPv4 Setup > DNS Server 1**.
  - Step 3** You should also verify that a CNAME entry was made in the DNS server for the TFTP server and for the Cisco Unified Communications Manager system.  
You must also ensure that DNS is configured to do reverse lookups.
- 

### Related Topics

[Phone Cannot Connect Using DNS, on page 169](#)

## Create a New Phone Configuration File

When you remove a phone from the Cisco Unified Communications Manager database, the configuration file is deleted from the Cisco Unified Communications Manager TFTP server. The phone directory number or numbers remain in the Cisco Unified Communications Manager database. They are called unassigned DN's and can be used for other devices. If unassigned DN's are not used by other devices, delete these DN's from the Cisco Unified Communications Manager database. You can use the Route Plan Report to view and delete unassigned reference numbers. For more information, see the documentation for your particular Cisco Unified Communications Manager release.

Changing the buttons on a phone button template, or assigning a different phone button template to a phone, may result in directory numbers that are no longer accessible from the phone. The directory numbers are still assigned to the phone in the Cisco Unified Communications Manager database, but the phone has no button on the phone with which calls can be answered. These directory numbers should be removed from the phone and deleted if necessary.

### Procedure

- 
- Step 1** From Cisco Unified Communications Manager, choose **Device > Phone** and click **Find** to locate the phone that is experiencing problems.
  - Step 2** Choose **Delete** to remove the phone from the Cisco Unified Communications Manager database.

**Note** When you remove a phone from the Cisco Unified Communications Manager database, the configuration file is deleted from the Cisco Unified Communications Manager TFTP server. The phone directory number or numbers remain in the Cisco Unified Communications Manager database. They are called unassigned DN's and can be used for other devices. If unassigned DN's are not used by other devices, delete these DN's from the Cisco Unified Communications Manager database. You can use the Route Plan Report to view and delete unassigned reference numbers.

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

**Step 4** Power cycle the phone.

#### Related Topics

[Phone Addition Methods](#), on page 47

## Determine DNS or Connectivity Issues

#### Procedure

**Step 1** Use the Reset Settings menu to reset phone settings to their default values.

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

- a) Disable DHCP.
- b) Assign static IP values to the phone. Use the same default router setting that other functioning phones use.
- c) Assign a TFTP server. Use the same TFTP server that other functioning phones use.

**Step 3** On the Cisco Unified Communications Manager server, verify that the local host files have the correct Cisco Unified Communications Manager server name mapped to the correct IP address.

**Step 4** From Cisco Unified Communications Manager, choose **System > Server** and verify that reference to the server is made by the IP address and not by the DNS name.

**Step 5** From Cisco Unified Communications Manager, choose **Device > Phone**. Click **Find** to search for this phone. Verify that you have assigned the correct MAC address to this Cisco IP Phone.

**Step 6** Power cycle the phone.

#### Related Topics

[Basic Reset](#), on page 187

[Determine the Phone MAC Address](#), on page 43

## Identify 802.1X Authentication Problems

#### Procedure

**Step 1** Verify that you have properly configured the required components.

**Step 2** Confirm that the shared secret is configured on the phone.

- If the shared secret is configured, verify that you have the same shared secret on the authentication server.
- If the shared secret is not configured on the phone, enter it, and ensure that it matches the shared secret on the authentication server.

## Start Service

A service must be activated before it can be started or stopped.

### Procedure

- 
- Step 1** From Cisco Unified Communications Manager Administration, choose **Cisco Unified Serviceability** from the Navigation drop-down list and click **Go**.
  - Step 2** Choose **Tools > Control Center - Feature Services**.
  - Step 3** Choose the primary Cisco Unified Communications Manager server from the Server drop-down list. The window displays the service names for the server that you chose, the status of the services, and a service control panel to start or stop a service.
  - Step 4** If a service has stopped, click the corresponding radio button and then click **Start**. The Service Status symbol changes from a square to an arrow.
- 

## Control Debug Information from Cisco Unified Communications Manager

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

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

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

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

- 7 - Debugging

Contact Cisco TAC for more information and assistance.

## Procedure

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

- **Device > Device settings > Common Phone Profile**
- **System > Enterprise Phone Configuration**
- **Device > Phone**

**Step 2** Set the following parameters:

- Log Profile - values: Preset (default), Default, Telephony
- Remote Log - values: Disable (default), Enable
- IPv6 Log Server or Log Server - IP address (IPv4 or IPv6 address)

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

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







## Maintenance

- [Basic Reset, page 187](#)
- [Voice Quality Monitoring, page 189](#)
- [Video Metrics, page 191](#)
- [Cisco IP Phone Cleaning, page 192](#)

### Basic Reset

Performing a basic reset of a Cisco Unified IP Phone provides a way to recover if the phone experiences an error and provides a way to reset or restore various configuration and security settings.

The following table describes the ways to perform a basic reset. You can reset a phone with any of these operations after the phone has started up. Choose the operation that is appropriate for your situation.

**Table 29: Basic Reset Methods**

Operation	Performing	Explanation
Restart phone	Press <b>Services, Applications</b> , or <b>Directories</b> and then press <b>**#**</b> .	Resets any user and network setup changes that you have made, but that the phone has not written to its flash memory, to previously saved settings, then restarts the phone.
Reset Settings	To reset settings, press <b>Applications</b> and choose <b>Administrator Settings &gt; Reset Settings &gt; Network</b> .	Resets user and network setup settings to their default values, and restarts the phone.
	To reset the CTL file, press <b>Applications</b> and choose <b>Administrator Settings &gt; Reset Settings &gt; Security</b> .	Resets the CTL file.

**Related Topics**

[Determine DNS or Connectivity Issues, on page 183](#)

[Factory Reset of Phone Has Deleted 802.1X Shared Secret, on page 176](#)

## Reset the Phone to the Factory Settings from the Phone Keypad

You can reset the phone to the factory settings. The reset clears all the phone parameters.

**Procedure**

- 
- Step 1** Remove power from the phone in one of these ways:
- Unplug the power adapter.
  - Unplug the LAN cable.
- Step 2** Press the pound (#) key and plug the phone in.
- Step 3** When the **Headset** and **Speaker** buttons are lit, enter the following key sequence:  
123456789\*0#
- The phone resets.
- 

## Perform Factory Reset from Phone Menu

To perform a factory reset of a phone,

**Procedure**

- 
- Step 1** Press **Applications**.
- Step 2** Choose **Administrator Settings > Reset Settings > All**.  
If required, unlock the phone options.
- 

**Related Topics**

[Apply a Phone Password, on page 31](#)

## Perform Network Configuration Reset

Resets network configuration settings to their default values and resets the phone. This method causes DHCP to reconfigure the IP address of the phone.

### Procedure

- 
- Step 1** From the **Administrator Settings** menu, if required, unlock phone options.
- Step 2** Choose **Reset Settings > Network Settings**.
- 

### Related Topics

[Apply a Phone Password, on page 31](#)

## Remove CTL File

Deletes only the CTL file from the phone.

### Procedure

- 
- Step 1** From the **Admin Settings** menu, if required, unlock phone options.
- Step 2** Choose **Reset Settings > Security**.
- 

### Related Topics

[Apply a Phone Password, on page 31](#)

## Voice Quality Monitoring

To measure the voice quality of calls that are sent and received within the network, Cisco IP Phones use these statistical metrics that are based on concealment events. The DSP plays concealment frames to mask frame loss in the voice packet stream.

- **Concealment Ratio metrics**—Show the ratio of concealment frames over total speech frames. An interval conceal ratio is calculated every 3 seconds.
- **Concealed Second metrics**—Show the number of seconds in which the DSP plays concealment frames due to lost frames. A severely “concealed second” is a second in which the DSP plays more than five percent concealment frames.



### Note

Concealment ratio and concealment seconds are primary measurements based on frame loss. A Conceal Ratio of zero indicates that the IP network is delivering frames and packets on time with no loss.

You can access voice quality metrics from the Cisco IP Phone using the Call Statistics screen or remotely by using Streaming Statistics.

## Voice Quality Troubleshooting Tips

When you observe significant and persistent changes to metrics, use the following table for general troubleshooting information.

**Table 30: Changes to Voice Quality Metrics**

Metric Change	Condition
Conceal Ratio and Conceal Seconds increase significantly	Network impairment from packet loss or high jitter.
Conceal Ratio is near or at zero, but the voice quality is poor.	<ul style="list-style-type: none"> <li>Noise or distortion in the audio channel such as echo or audio levels.</li> <li>Tandem calls that undergo multiple encode/decode such as calls to a cellular network or calling card network.</li> <li>Acoustic problems coming from a speakerphone, handsfree cellular phone or wireless headset.</li> </ul> <p>Check packet transmit (TxCnt) and packet receive (RxCnt) counters to verify that voice packets are flowing.</p>
MOS LQK scores decrease significantly	<p>Network impairment from packet loss or high jitter levels:</p> <ul style="list-style-type: none"> <li>Average MOS LQK decreases may indicate widespread and uniform impairment.</li> <li>Individual MOS LQK decreases may indicate bursty impairment.</li> </ul> <p>Cross-check the conceal ratio and conceal seconds for evidence of packet loss and jitter.</p>
MOS LQK scores increase significantly	<ul style="list-style-type: none"> <li>Check to see if the phone is using a different codec than expected (RxType and TxType).</li> <li>Check to see if the MOS LQK version changed after a firmware upgrade.</li> </ul>


**Note**

Voice quality metrics do not account for noise or distortion, only frame loss.

## Voice Quality Metrics

When using 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 also important to distinguish significant changes from random changes in metrics. Significant changes are scores that change about 0.2 MOS or more and persist in calls that last longer than 30 seconds. Conceal ratio changes indicate a frame loss greater than 3 percent.

The MOS LQK scores can vary based on the codec that the Cisco Unified IP Phone uses. The following codecs provide these corresponding maximum MOS LQK scores under normal conditions with zero frame loss for Cisco Unified Phone 8941 and 8945:

- G.711: 4.5 MOS LQK
- G.722: 4.5 MOS LQK
- G.728/iLBC: 3.9 MOS LQK
- G729A/AB: 3.7 MOS LQK


**Note**

- Cisco Voice Transmission Quality (CVTQ) does not support wideband (7 kHz) speech codecs, because ITU has not defined the extension of the technique to wideband. Therefore, MOS LQK scores that correspond to G.711 performance are reported for G.722 calls to allow basic quality monitoring, rather than not reporting an MOS score.
- Reporting G.711-scale MOS scores for wideband calls through the use of CVTQ allows basic-quality classifications to be indicated as good/normal or bad/abnormal. Calls with high scores (approximately 4.5) indicate high quality or a low packet loss, and lower scores (approximately 3.5) indicate low quality or a high packet loss.
- Unlike MOS, the conceal ratio and concealed seconds metrics remain valid and useful for both wideband and narrowband calls.

A conceal ratio of zero indicates that the IP network is delivering frames and packets on time with no loss.

## Video Metrics

The phones do not support video metrics. This means that you can't see the following information about the video portion of a call:

- videoContentType
- videoDuration
- numberVideoPacketsSent
- numberVideoOctetsSent
- numberVideoPacketsReceived
- numberVideoOctetsReceived
- numberVideoPacketsLost
- videoAverageJitter

## Cisco IP Phone Cleaning

To clean your Cisco IP Phone, use only a dry soft cloth to gently wipe the phone and the phone screen. Do not apply liquids or powders directly to the phone. As with all non-weatherproof electronics, liquids and powders can damage the components and cause failures.

When the phone is in sleep mode, the screen is blank and the Select button is not lit. When the phone is in this condition, you can clean the screen, as long as you know that the phone will remain asleep until after you finish cleaning.



## International User Support

- [Unified Communications Manager Endpoints Locale Installer](#), page 193
- [International Call Logging Support](#), page 193
- [Language Limitation](#), page 194

### Unified Communications Manager Endpoints Locale Installer

By default, Cisco IP Phones are set up for the English (United States) locale. To use the Cisco IP Phones in other locales, you must install the locale-specific version of the Unified Communications Manager Endpoints Locale Installer on every Cisco Unified Communications Manager server in the cluster. The Locale Installer installs the latest translated text for the phone user interface and country-specific phone tones on your system so that they are available for the Cisco IP Phones.

To access the Locale Installer required for a release, access <https://software.cisco.com/download/navigator.html?mdfid=286037605&flowid=46245>, navigate to your phone model, and select the Unified Communications Manager Endpoints Locale Installer link.

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



#### Note

The latest Locale Installer may not be immediately available; continue to check the website for updates.

### International Call Logging Support

If your phone system is configured for international call logging (calling party normalization), the call logs, redial, or call directory entries may display a plus (+) symbol to represent the international escape code for your location. Depending on the configuration for your phone system, the + may be replaced with the correct international dialing code, or you may need to edit the number before dialing to manually replace the + with the international escape code for your location. In addition, while the call log or directory entry may display the full international number for the received call, the phone display may show the shortened local version of the number, without international or country codes.

## Language Limitation

There is no localized Keyboard Alphanumeric Text Entry (KATE) support for the following Asian locales:

- Chinese (China)
- Chinese (Hong Kong)
- Chinese (Taiwan)
- Japanese (Japan)
- Korean (Korea Republic)

The default English (United States) KATE is presented to the user instead.

For example, the phone screen will show text in Korean, but the **2** key on the keypad will display a b c 2 A B C.