



## **Cisco IP Phone 7821, 7841, and 7861 Administration Guide for Cisco Unified Communications Manager 10.0 (SIP)**

**First Published:** October 25, 2013

**Last Modified:** November 12, 2013

### **Americas Headquarters**

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

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)

© 2013 Cisco Systems, Inc. All rights reserved.



## CONTENTS

---

### Preface

#### Preface **xiii**

Overview **xiii**

Audience **xiii**

Guide conventions **xiii**

Related documentation **xv**

    Cisco IP Phone 7800 Series documentation **xv**

    Cisco Unified Communications Manager documentation **xv**

    Cisco Business Edition 3000 documentation **xv**

    Cisco Business Edition 6000 documentation **xv**

Documentation, support, and security guidelines **xv**

    Cisco product security overview **xvi**

---

### PART I

#### About the Cisco 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 **6**

    Power reduction **7**

Supported network protocols **7**

VLAN interaction **11**

Cisco Unified Communications Manager interaction **12**

Cisco Unified Communications Manager Express interaction **12**

External devices 13

---

**CHAPTER 2****Cisco IP Phone hardware 15**

Cisco IP phone hardware overview 15

Cisco IP Phone 7821 16

Phone connections 16

Buttons and hardware 17

Cisco IP Phone 7841 20

Phone connections 20

Buttons and hardware 21

Cisco IP Phone 7861 23

Phone connections 23

Buttons and hardware 25

Terminology differences 27

---

**PART II****Cisco IP Phone Installation 29**

---

**CHAPTER 3****Cisco IP Phone installation 31**

Verify network setup 31

Enable autoregistration for phone 32

Install Cisco IP Phone 33

Set up phone from setup menus 35

Apply phone password 36

Text and menu entry from phone 36

Configure network settings 37

Set Domain Name field 37

Set Admin VLAN ID field 38

Set PC VLAN field 38

Set SW Port Configuration field 38

Set PC Port Configuration field 38

Set DHCP Enabled field 39

Set IP Address field 39

Set Subnet Mask field 39

Set Default Router field 39

Set DNS Server fields 40

- Set Alternate TFTP field 40
- Set TFTP Server 1 field 40
- Set TFTP Server 2 field 41
- Verify phone startup 41
- Configure Phone Services for users 41

---

**CHAPTER 4****Cisco Unified Communications Manager phone setup 43**

- Determine phone MAC address 43
- Set up Cisco IP Phone 43
- Phone addition methods 48
  - Add phones individually 48
  - Add phones using BAT phone template 49
- Add users to Cisco Unified Communications Manager 49
  - Add user from external LDAP directory 50
  - Add user directly to Cisco Unified Communications Manager 50
- Add user to End User group 51
- Associate phones with users 51

---

**CHAPTER 5****Self Care Portal management 53**

- Self Care Portal overview 53
- Set up access to Self Care Portal 53
- Customize Self Care Portal display 54

---

**PART III****Hardware and accessory installation 55**

---

**CHAPTER 6****Cisco IP Phone accessories 57**

- Cisco IP phone accessories overview 57
- Connect footstand 58
- Secure the phone with cable lock 59
- Headsets 59
  - Audio quality 60
  - Analog headsets 60
    - Enable wideband on analog headsets 60
    - Enable wideband codec on analog headsets 60
  - Wired headsets 61

Connect wired headset 61

Disable wired headset 61

---

**CHAPTER 7**

**Wall Mounts 63**

Non-lockable wall mount components 63

Install non-lockable wall mount kit 65

Remove phone from non-lockable wall mount 70

Adjust handset rest 71

---

**PART IV**

**Cisco IP Phone Administration 73**

---

**CHAPTER 8**

**Cisco IP Phone security 75**

Cisco IP phone security overview 75

View current security features on phone 76

View Security Profiles 76

Supported security features 76

Set up Locally Significant Certificate 78

Phone call security 79

Secure Conference Call Identification 80

Secure Phone Call Identification 81

Provide encryption for Barge 81

802.1X authentication 82

---

**CHAPTER 9**

**Cisco IP Phone customization 85**

Custom phone rings 85

Set Up Custom Phone Ring 85

Custom ring file formats 86

Set up wideband codec 87

Set up idle display 88

---

**CHAPTER 10**

**Phone Features and Setup 89**

Cisco IP Phone user support 90

Telephony features for Cisco IP Phone 90

Feature buttons and softkeys 107

Create Feature Control Policy 109

Feature Control Policy default values	110
Disable speakerphone	111
Schedule Power Save for Cisco IP Phone	111
Schedule Power Save Plus (EnergyWise) on Cisco IP Phone	112
Enable Agent Greeting	115
Set up Do Not Disturb	116
Set up monitoring and recording	117
Set up Power Negotiation for LLDP	117
Set up cBarge	118
Set up Automatic Port Synchronization	118
Set up SSH Access	119
Set up Call Forward Notification	119
Set up Client Matter Codes	120
Enable Line Status for Call Lists	121
Set up Forced Authorization Codes	121
Set up Incoming Call Toast Timer	122
Set up Peer Firmware Sharing	122
Set up Remote Port Configuration	123
Enable Device Invoked Recording	124
Set Headset Sidetone Control	124
Enable Actionable Incoming Call Alert	125
Enable Call History for Shared Line	126
Control phone web page access	126
UCR 2008 setup	127
Set up UCR 2008 in Common Device Configuration	128
Set up UCR 2008 in Common Phone Profile	128
Set up UCR 2008 in Enterprise Phone Configuration	128
Set up UCR 2008 in Phone	129
Set up softkey template	129
Set minimum ring volume	132
Set up Join and Direct Transfer Policy	132
Set up HTTPS for Phone Services	133
Phone button templates	133
Modify phone button template	133
Assign phone button template for All Calls	134

- Set up PAB or Speed Dial as IP phone service 134
- Modify phone button template for PAB or Fast Dial 135

---

**CHAPTER 11**

**Corporate and Personal Directory setup 137**

- Corporate Directory setup 137
- Personal Directory setup 137
- User personal directory entries setup 138
  - Download Cisco IP Phone Address Book Synchronizer 138
  - Cisco IP Phone Address Book Synchronizer deployment 138
    - Install synchronizer 139
    - Set up synchronizer 139

---

**PART V**

**Cisco IP Phone Troubleshooting 141**

---

**CHAPTER 12**

**Monitoring phone systems 143**

- Monitoring phone systems overview 143
- Cisco IP Phone status 143
  - Display Model Information window 144
  - Display Status menu 144
    - Display Status Messages window 144
      - Status messages fields 145
    - Display Network Statistics window 150
      - Network Statistics fields 150
    - Display Call Statistics window 152
      - Call Statistics fields 152
    - Display Security Configuration window 154
      - Security Configuration fields 154
- Cisco IP Phone web page 155
  - Access Web Page for phone 155
    - Device information 156
    - Network setup 157
    - Network statistics 161
      - Ethernet Information web page 161
      - Access Area and Network Area web pages 162
  - Device Logs 164



Streaming Statistics 164

---

**CHAPTER 13****Troubleshooting 169**

General troubleshooting information 169

Startup problems 171

    Cisco IP Phone does not go through normal startup process 171

    Cisco IP Phone does not register with Cisco Unified Communications Manager 172

    Phone displays error messages 172

        Phone cannot connect to TFTP server or to Cisco Unified Communications Manager  
        172

        Phone cannot connect to TFTP server 172

        Phone cannot connect to server 173

        Phone cannot connect using DNS 173

    Cisco Unified Communications Manager and TFTP services are not running 173

    Configuration file corruption 174

    Cisco Unified Communications Manager phone registration 174

    Cisco IP Phone cannot obtain IP address 174

Cisco IP Phone reset problems 174

    Phone resets due to intermittent network outages 175

    Phone resets due to DHCP setting errors 175

    Phone resets due to incorrect static IP address 175

    Phone resets during heavy network usage 175

    Phone resets due to intentional reset 176

    Phone resets due to DNS or other connectivity issues 176

    Phone does not power up 176

Phone cannot connect to LAN 176

Cisco IP Phone security problems 177

    CTL file problems 177

        Authentication error, phone cannot authenticate CTL file 177

        Phone cannot authenticate CTL file 177

        CTL file authenticates but other configuration files do not authenticate 177

        ITL file authenticates but other configuration files do not authenticate 178

        TFTP authorization fails 178

        Phone does not register 178

        Signed configuration files are not requested 179

802.1X authentication problems	179
802.1X enabled on phone but phone does not authenticate	180
802.1X is not enabled	180
Factory reset of phone has deleted 802.1X Shared Secret	180
Audio and video problems	181
Phone display is wavy	181
No audio	181
No speech path	181
Choppy speech	182
General telephone call problems	182
Phone call cannot be established	182
Phone does not recognize DTMF digits or digits are delayed	183
Troubleshooting procedures	183
Check TFTP settings	183
Determine DNS or connectivity issues	183
Check DHCP settings	184
Create new phone configuration file	185
Identify 802.1X authentication problems	185
Verify DNS settings	186
Start service	186
Troubleshoot using Debug menu	187
Additional troubleshooting information	188

---

**CHAPTER 14****Maintenance 189**

Basic reset	189
Perform factory reset from phone keypad	190
Perform factory reset from phone menu	190
Perform network configuration reset	191
Perform user and network configuration reset	191
Remove CTL file	191
Quality Report Tool	192
Voice quality monitoring	192
Voice quality troubleshooting tips	193
Cisco IP Phone cleaning	194

---

**CHAPTER 15**

**International User Support 195**

Unified Communications Manager Endpoints Locale Installer **195**

International Call Logging support **195**





## Preface

---

- [Overview](#), page [xiii](#)
- [Audience](#), page [xiii](#)
- [Guide conventions](#), page [xiii](#)
- [Related documentation](#), page [xv](#)
- [Documentation, support, and security guidelines](#), page [xv](#)

## Overview

*Cisco IP Phone 7821, 7841, and 7861 Administration Guide for Cisco Unified Communications Manager (SIP)* provides the information you need to understand, install, configure, manage, and troubleshoot the phones on a VoIP network.

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

## Audience

Network engineers, system administrators, and telecom engineers should review this guide to learn the steps that are required to set up Cisco 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 IP Phone 7800 Series documentation

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

[http://www.cisco.com/en/US/products/ps13220/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps13220/tsd_products_support_series_home.html)

### Cisco Unified Communications Manager documentation

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

[http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html)

### Cisco Business Edition 3000 documentation

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

[http://www.cisco.com/en/US/products/ps11370/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps11370/tsd_products_support_series_home.html)

### Cisco Business Edition 6000 documentation

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

[http://www.cisco.com/en/US/products/ps11369/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps11369/tsd_products_support_series_home.html)

## Documentation, support, and security guidelines

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

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

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

## Cisco product security overview

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

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





## PART **I**

# About the Cisco IP Phone

- [Technical details, page 3](#)
- [Cisco IP Phone hardware, page 15](#)





# CHAPTER 1

## Technical details

- [Physical and operating environment specifications, page 3](#)
- [Cable specifications, page 4](#)
- [Network and computer port pinouts, page 4](#)
- [Phone power requirements, page 6](#)
- [Supported network protocols, page 7](#)
- [VLAN interaction, page 11](#)
- [Cisco Unified Communications Manager interaction, page 12](#)
- [Cisco Unified Communications Manager Express interaction, page 12](#)
- [External devices, page 13](#)

## Physical and operating environment specifications

The following table shows the physical and operating environment specifications for the Cisco IP Phone 7821, 7841, and 7861.

**Table 1: Physical and operating specifications**

Specification	Value or range
Operating temperature	23° to 113°F (–5° to 45°C)
Operating relative humidity	10% to 90% (noncondensing)
Storage temperature	–13° to 176°F (–25° to 80°C)
Height	7.3 in. (18.57 cm)
Width	5.8 in. (14.79 cm)

Specification	Value or range
Depth	7.1 in. (18.05 cm)
Weight	2.2 lb (1.0 kg)
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 3/5/5e for 10-Mbps cables with 4 pairs Category 5/5e 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 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 (on Cisco IP Phones 7821 and 7861) and the LAN 1000BaseT connection (on the Cisco IP Phone 7841).
- RJ-45 jack for a second 10/100BaseT compliant connection (on Cisco IP Phones 7821 and 7861) and the LAN 1000BaseT connection (on the Cisco IP Phone 7841).
- 48-volt power connector.

## Network and computer port pinouts

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

- The network port is the 10/100 SW port (The Cisco IP Phone 7841 has a 10/100/1000 SW network port).
- The computer (access) port is the 10/100 PC port (The Cisco IP Phone 7841 has a 10/100/1000 PC computer port).

### 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 IP Phone 7821, 7841, and 7861 can be powered with external power or with Power over Ethernet (PoE). A separate power supply provides external power. The switch can provide PoE through the phone Ethernet cable.



### Note

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

The following table provides guidelines for Cisco IP Phone 7821, 7841, and 7861 power.

**Table 4: Guidelines for Cisco IP Phone 7821, 7841, and 7861 power**

Power type	Guidelines
External power: Provided through the CP-PWR-CUBE-4= external power supply	The Cisco IP Phone 7821, 7841, and 7861 uses the CP-PWR-CUBE-4 power supply.
External power—Provided through the Cisco IP Phone Power Injector.	The Cisco IP Phone Power Injector may be used with any Cisco IP Phone. Functioning as a midspan device, the injector delivers inline power to the attached phone. The Cisco IP Phone Power Injector connects between a switch port and the IP Phone, and supports a maximum cable length of 100m between the unpowered switch and the IP phone.
PoE power—Provided by a switch through the Ethernet cable attached to the phone.	<p>Cisco IP Phone 7821, 7841, and 7861 supports IEEE 802.3af Class 3 power on signal pairs and spare pairs.</p> <p>Cisco IP Phone 7821, 7841, and 7861 supports IEEE 802.3at for external add-on devices.</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 that runs on your switch supports your intended phone deployment. See the documentation for your switch for operating system version information.</p> <p>Support for NG-PoE+: The Cisco IP Phone 7821, 7841, and 7861 can draw more power than IEEE 802.3at, as long as there is NG-PoE+ switch support.</p>

## Power outage

Power outages and other devices can affect your Cisco IP Phone.

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

## Power reduction

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

### Power Save

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

Set up each phone to enable or disable Power Save settings. You can configure the phones to dim the backlight on a schedule.

### Power Save Plus (EnergyWise)

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

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

### Related Topics

[Schedule Power Save Plus \(EnergyWise\) on Cisco IP Phone, on page 112](#)

[Schedule Power Save for Cisco IP Phone, on page 111](#)

## Supported network protocols

Cisco 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 IP Phone 7821, 7841, and 7861 support.

**Table 5: Supported network protocols on the Cisco IP Phone**

Network protocol	Purpose	Usage notes
Bootstrap Protocol (BootP)	BootP enables a network device such as the Cisco IP Phone to discover certain startup information, such as its IP address.	—

Network protocol	Purpose	Usage notes
Cisco Audio Session Tunneling (CAST)	The CAST protocol allows IP phones and associated applications behind the phone to discover and communicate with the remote endpoints without requiring changes to the traditional signaling components like Cisco Unified Communications Manager and gateways. The CAST protocol allows separate hardware devices to synchronize related media and it allows PC applications to augment nonvideo-capable phones to become video enabled using the PC as the video resource.	—
Cisco Discovery Protocol (CDP)	CDP is a device-discovery protocol that runs on all Cisco-manufactured equipment.  Using CDP, a device can advertise its existence to other devices and receive information about other devices in the network.	The Cisco 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.
Dynamic Host Configuration Protocol (DHCP)	DHCP dynamically allocates and assigns an IP address to network devices.  DHCP enables you to connect an IP phone into the network and have the phone become operational without your needing to manually assign an IP address or to configure additional network parameters.	DHCP is enabled by default. If disabled, you must manually configure the IP address, subnet mask, gateway, and a TFTP server on each phone locally.  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> .  <b>Note</b> If you cannot use option 150, you may try using DHCP option 66.
Hypertext Transfer Protocol (HTTP)	HTTP is the standard way of transferring information and moving documents across the Internet and the web.	Cisco IP Phones use HTTP for the XML services and for troubleshooting purposes.



Network protocol	Purpose	Usage notes
Hypertext Transfer Protocol Secure (HTTPS)	<p>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.</p> <p><b>Note</b> IP phones can be HTTPS clients; they cannot be HTTPS servers.</p>	<p>Web applications with both HTTP and HTTPS support have two URLs configured. Cisco IP Phones that support HTTPS choose the HTTPS URL.</p> <p>A lock icon is displayed to the user if the connection to the service is via HTTPS.</p>
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 IP Phone implements the IEEE 802.1X standard by providing support for the following authentication methods: EAP-FAST and EAP-TLS.</p> <p>When 802.1X authentication is enabled on the phone, you should disable the PC port and voice VLAN. Refer to the <a href="#">802.1X authentication, on page 82</a> for additional information.</p>
Internet Protocol (IP)	<p>IP is a messaging protocol that addresses and sends packets across the network.</p>	<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 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> <p>The Cisco IP Phones support IPv6 address. For more information, see “Internet Protocol Version 6 (IPv6)” in the <i>Cisco Unified Communications Manager Features and Services Guide</i>.</p>
Link Layer Discovery Protocol (LLDP)	<p>LLDP is a standardized network discovery protocol (similar to CDP) that is supported on some Cisco and third-party devices.</p>	<p>The Cisco IP Phone supports LLDP on the PC port.</p>

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 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 <i>LLDP-MED and 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 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 enabled by default.
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.	<p>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.</p> <p>You can configure the Cisco IP Phone to use SIP.</p>
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 IP Phones use SRTP for media encryption.

Network protocol	Purpose	Usage notes
Transmission Control Protocol (TCP)	TCP is a connection-oriented transport protocol.	Cisco IP Phones use TCP to connect to Cisco Unified Communications Manager and to access XML services.
Transport Layer Security (TLS)	TLS is a standard protocol for securing and authenticating communications.	When security is implemented, Cisco IP Phones use the TLS protocol when securely registering with Cisco Unified Communications Manager.  For more information, see <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 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 “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 IP Phones transmit and receive RTP streams, which utilize UDP.

### Related Topics

[Verify network setup, on page 31](#)

[Verify phone startup, on page 41](#)

## VLAN interaction

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

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

- The current VLANs might be configured on an IP subnet basis. However, additional IP addresses might not be available to assign the phone to the same subnet as other devices that connect to the same port.

- Data traffic present on the VLAN supporting phones might reduce the quality of VoIP traffic.
- Network security may indicate a need to isolate the VLAN voice traffic from the VLAN data traffic.

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

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

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

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

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

## Cisco Unified Communications Manager interaction

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

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

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



### 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, go to the following URL and install the latest support patch for your version of Cisco Unified Communications Manager:

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

## Cisco Unified Communications Manager Express interaction

When the Cisco IP Phone works with the Cisco Unified Communications Manager Express, 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.

Users cannot create conference and transfer calls across different lines.

## External devices

We recommend using good-quality external devices, such as headsets, cables, and connectors, that are shielded against unwanted radio frequency (RF) and audio frequency (AF) signals.

**Note**

Not all Cisco IP Telephony products support external devices, cords or cables. For more information, consult the documentation for your phone.

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

---



## Cisco IP Phone hardware

---

- [Cisco IP phone hardware overview, page 15](#)
- [Cisco IP Phone 7821, page 16](#)
- [Cisco IP Phone 7841, page 20](#)
- [Cisco IP Phone 7861, page 23](#)
- [Terminology differences, page 27](#)

### Cisco IP phone hardware overview

The Cisco IP Phone 7821, 7841, and 7861 provides voice communication over an Internet Protocol (IP) network. The Cisco IP Phone functions much like a digital business phone, allowing you to place and receive phone calls and to access features such as mute, hold, transfer, speed dial, call forward, and more. In addition, because the phone connects to your data network, it offers enhanced IP telephony features, including access to network information and services, and customizable features and services.

The Cisco IP Phones have the following features:

- Programmable feature buttons that support up to 16 lines (Cisco IP Phone 7821 supports 2 lines, Cisco IP Phone 7841 supports 4 lines and Cisco IP phone 7861 supports 16 lines) or that can be programmed for other features
- Gigabit ethernet connectivity (This is applicable only to Cisco IP Phone 7841)
- Support for an external microphone and speakers

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



**Caution**

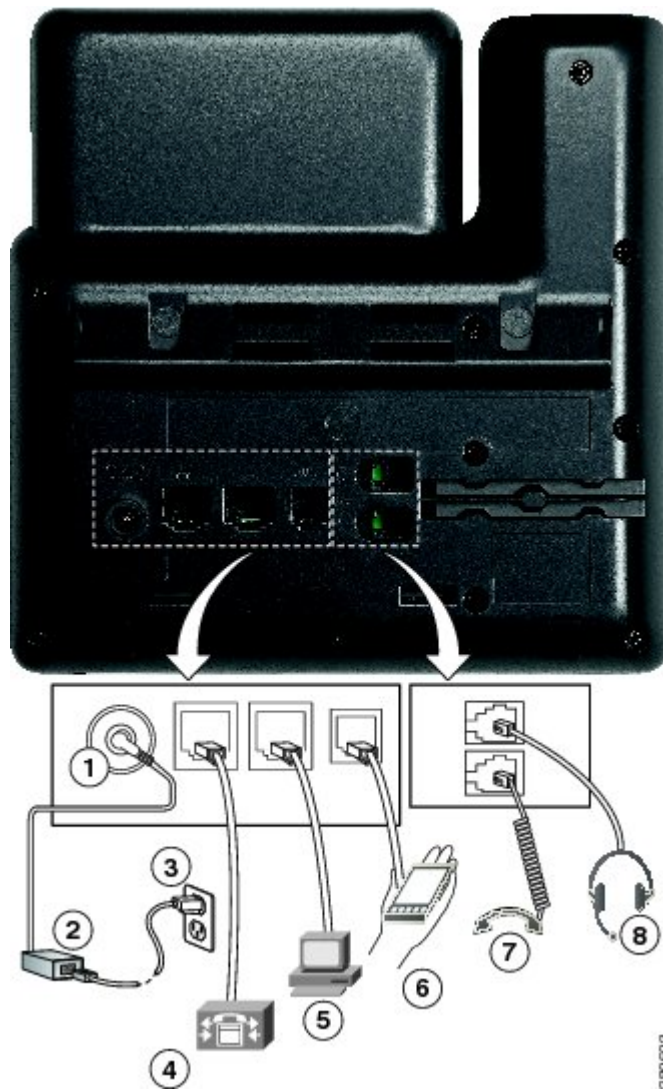
Using a cell, mobile, or GSM phone, or two-way radio in close proximity to a Cisco IP Phone might cause interference. For more information, see the manufacturer's documentation of the interfering device.

---

# Cisco IP Phone 7821

## Phone connections

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

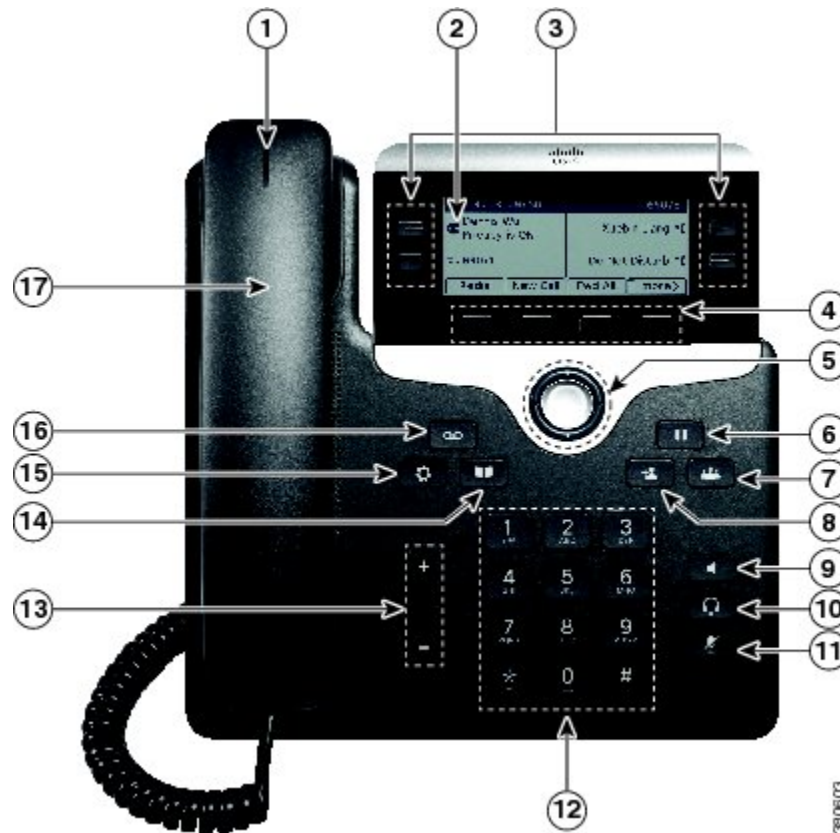


1	DC adaptor port (DC48V).	5	Access port (10/100 PC) connection.
2	AC-to-DC power supply (optional).	6	Auxiliary port.
3	AC power wall plug (optional).	7	Handset connection.

















4	Network port (10/100 SW) connection. IEEE 802.3af power enabled.	8	Analog headset connection (optional).
---	--	---	---------------------------------------

## Buttons and hardware



1	Handset light strip	Indicates an incoming call (flashing red) or new voice message (steady red).
2	Phone screen	Shows information about your phone such as directory number, active call and line status, softkey options, speed dials, placed calls, and phone menu listings.

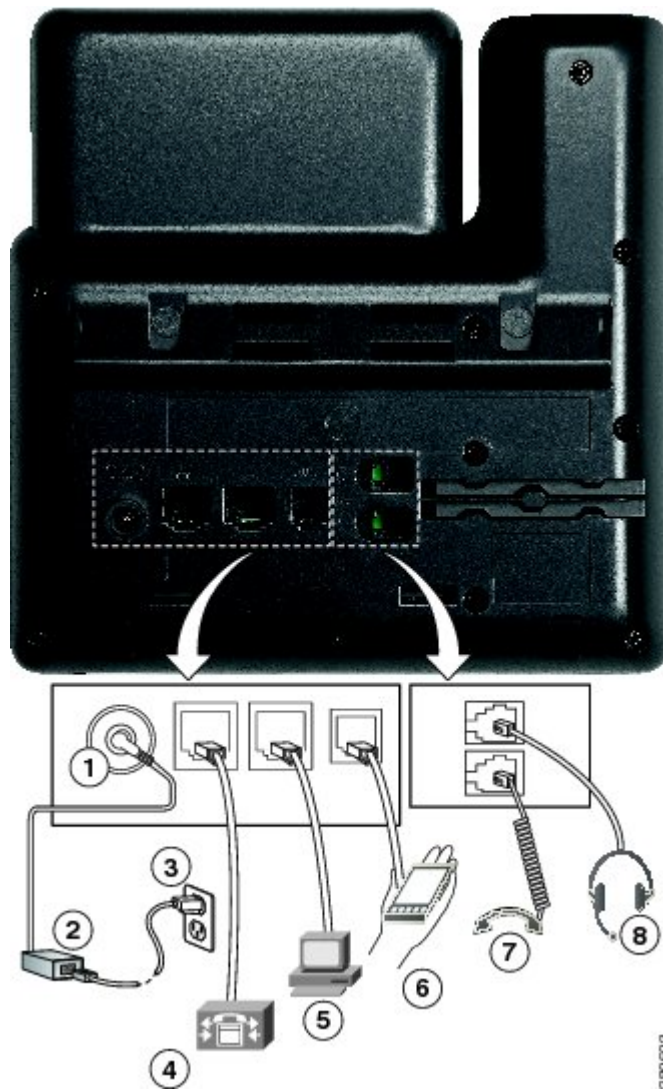
3	Programmable feature buttons 	Depending on how your system administrator sets up the phone, programmable feature buttons (on each side of the phone screen) provide access to: <ul style="list-style-type: none"> <li>• Phone lines and intercom lines</li> <li>• Speed-dial numbers (speed-dial buttons, including the Line Status speed-dial features)</li> <li>• Web-based services (for example, a Personal Address Book button)</li> <li>• Call features (for example, a Privacy button)</li> </ul> Buttons illuminate to indicate status: <ul style="list-style-type: none"> <li>• Green, steady: Active call or two-way intercom call</li> <li>• Green, flashing: Held call</li> <li>• Amber, steady: Privacy in use, one-way intercom call, DND active, or logged into Hunt Group</li> <li>• Amber, flashing: Incoming call or reverting call</li> <li>• Red, steady: Remote line in use (shared line or Line Status)</li> <li>• Red, flashing: Remote line on hold</li> </ul>
4	Softkey buttons 	Depending on how your system administrator sets up the phone, enable softkey options displayed on your phone screen.
5	Navigation and Select button 	The Navigation and Select button allows you to scroll through menus, highlight items and select the highlighted item.
6	Hold button 	Places an active call on hold.
7	Conference button 	Creates a conference call.
8	Transfer button 	Transfers a call.
9	Speakerphone button 	Toggles the speakerphone on or off. When the speakerphone is on, the button is lit.

10	Headset button 	Toggles the headset on or off. When the headset is on, the button is lit.
11	Mute button 	Toggles the microphone on or off. When the microphone is muted, the button is lit.
12	Keypad	Allows you to dial phone numbers, enter letters, and select menu items (by entering the item number).
13	Volume button 	Controls the handset, headset, and speakerphone volume (off hook) and the ringer volume (on hook).
14	Volume button 	Opens or closes the Directories menu. Use the Contacts button to access personal and corporate directories.
14	Messages button 	Autodials your voice messaging system (varies by system).
15	Applications button 	Opens or closes the Applications menu. Use the Applications button to access call history, user preferences, phone settings, and phone model information.
16	Messages button 	Autodials your voice messaging system (varies by system).
17	Handset	Phone handset.

# Cisco IP Phone 7841

## Phone connections

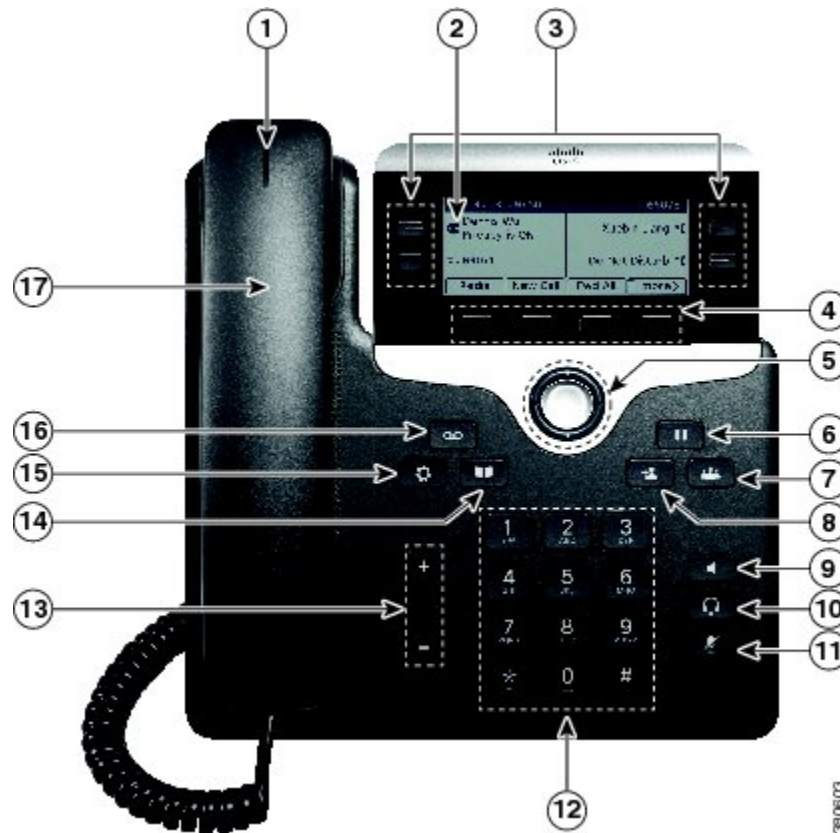
For your phone to work, it must be connected to the corporate IP telephony network.










1	DC adaptor port (DC48V).	5	Access port (10/100/1000 PC) connection.
2	AC-to-DC power supply (optional).	6	Auxiliary port.
3	AC power wall plug (optional).	7	Handset connection.







4	Network port (10/100/1000 SW) connection. IEEE 802.3af power enabled.	8	Analog headset connection (optional).
---	---	---	---------------------------------------

## Buttons and hardware



1	Handset light strip	Indicates an incoming call (flashing red) or new voice message (steady red).
2	Phone screen	Shows information about your phone such as directory number, active call and line status, softkey options, speed dials, placed calls, and phone menu listings.

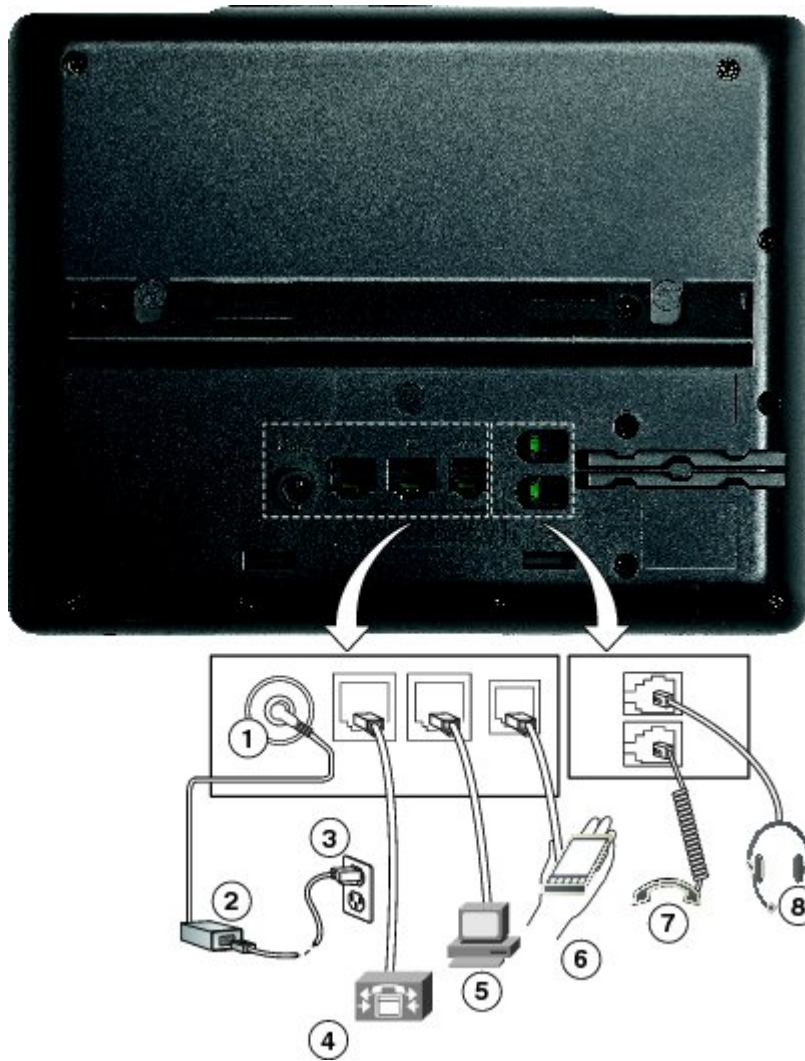
3	Programmable feature buttons 	<p>Depending on how your system administrator sets up the phone, programmable feature buttons (on each side of the phone screen) provide access to:</p> <ul style="list-style-type: none"> <li>• Phone lines and intercom lines</li> <li>• Speed-dial numbers (speed-dial buttons, including the Line Status speed-dial features)</li> <li>• Web-based services (for example, a Personal Address Book button)</li> <li>• Call features (for example, a Privacy button)</li> </ul> <p>Buttons illuminate to indicate status:</p> <ul style="list-style-type: none"> <li>• Green, steady: Active call or two-way intercom call</li> <li>• Green, flashing: Held call</li> <li>• Amber, steady: Privacy in use, one-way intercom call, DND active, or logged into Hunt Group</li> <li>• Amber, flashing: Incoming call or reverting call</li> <li>• Red, steady: Remote line in use (shared line or Line Status)</li> <li>• Red, flashing: Remote line on hold</li> </ul>
4	Softkey buttons 	Depending on how your system administrator sets up the phone, enable softkey options displayed on your phone screen.
5	Navigation and Select button 	The Navigation and Select button allows you to scroll through menus, highlight items and select the highlighted item.
6	Hold button 	Places an active call on hold.
7	Conference button 	Creates a conference call.
8	Transfer button 	Transfers a call.
9	Speakerphone button 	Toggles the speakerphone on or off. When the speakerphone is on, the button is lit.

10	Headset button 	Toggles the headset on or off. When the headset is on, the button is lit.
11	Mute button 	Toggles the microphone on or off. When the microphone is muted, the button is lit.
12	Keypad	Allows you to dial phone numbers, enter letters, and select menu items (by entering the item number).
13	Volume button 	Controls the handset, headset, and speakerphone volume (off hook) and the ringer volume (on hook).
14	Contacts button 	Opens or closes the Directories menu. Use the Contacts button to access personal and corporate directories.
15	Applications button 	Opens or closes the Applications menu. Use the Applications button to access call history, user preferences, phone settings, and phone model information.
16	Messages button 	Autodials your voice messaging system (varies by system).
17	Handset	Phone handset.

## Cisco IP Phone 7861

### Phone connections

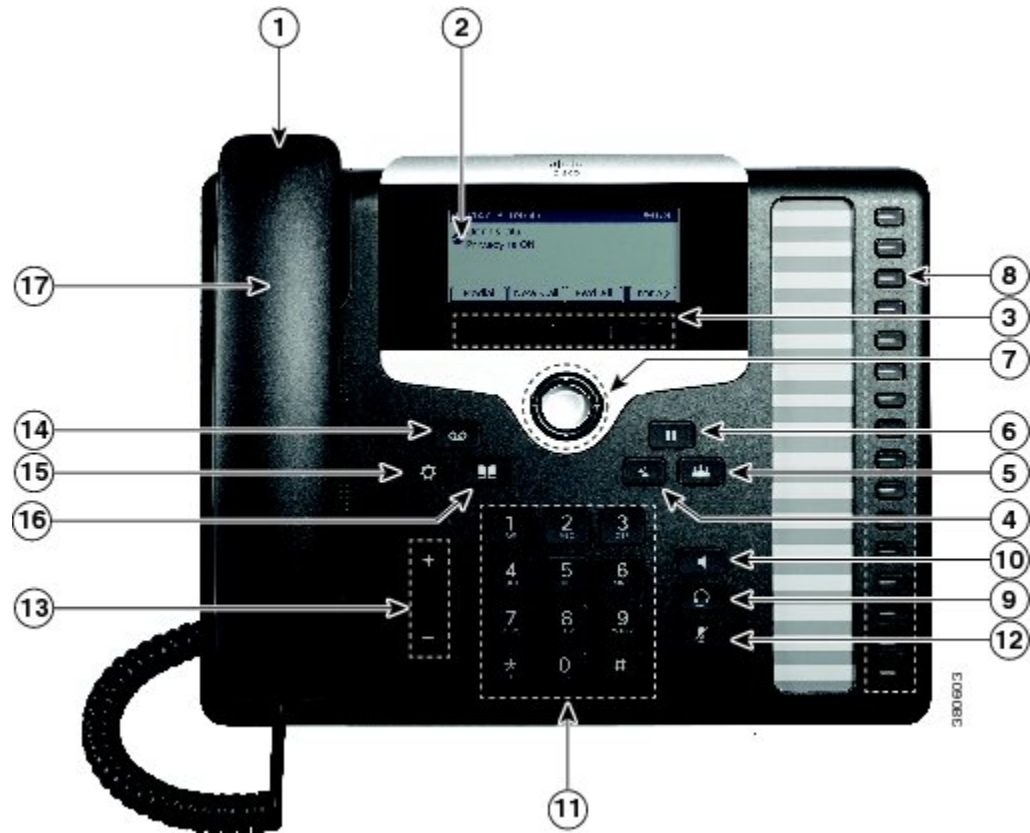
For your phone to work, it must be connected to the corporate IP telephony network.











1	DC adaptor port (DC48V).	5	Access port (10/100 PC) connection.
2	AC-to-DC power supply (optional).	6	Auxiliary port.
3	AC power wall plug (optional).	7	Handset connection.
4	Network port (10/100 SW) connection. IEEE 802.3af power enabled.	8	Analog headset connection (optional).








## Buttons and hardware



1	Handset light strip	Indicates an incoming call (flashing red) or new voice message (steady red).
2	Phone screen	Shows information about your phone such as directory number, active call and line status, softkey options, speed dials, placed calls, and phone menu listings.
3	Softkey buttons 	Depending on how your system administrator sets up the phone, enable softkey options displayed on your phone screen.
4	Transfer button 	Transfers a call.

5	Conference button 	Creates a conference call.
6	Hold button 	Places an active call on hold.
7	Navigation and Select button 	The Navigation and Select button allows you to scroll through menus, highlight items and select the highlighted item.
8	Programmable feature buttons 	<p>Depending on how your system administrator sets up the phone, programmable feature buttons provide access to:</p> <ul style="list-style-type: none"> <li>• Phone lines and intercom lines</li> <li>• Speed-dial numbers (speed-dial buttons, including the Line Status speed-dial features)</li> <li>• Web-based services (for example, a Personal Address Book button)</li> <li>• Call features (for example, a Privacy button)</li> </ul> <p>Buttons illuminate to indicate status:</p> <ul style="list-style-type: none"> <li>• Green, steady: Active call or two-way intercom call</li> <li>• Green, flashing: Held call</li> <li>• Amber, steady: Privacy in use, one-way intercom call, DND active, or logged into Hunt Group</li> <li>• Amber, flashing: Incoming call or reverting call</li> <li>• Red, steady: Remote line in use (shared line or Line Status)</li> <li>• Red, flashing: Remote line on hold</li> </ul>
9	Headset button 	Toggles the headset on or off. When the headset is on, the button is lit.
10	Speakerphone button 	Toggles the speakerphone on or off. When the speakerphone is on, the button is lit.
11	Keypad	Allows you to dial phone numbers, enter letters, and select menu items (by entering the item number).

12	Mute button 	Toggles the microphone on or off. When the microphone is muted, the button is lit.
13	Volume button 	Controls the handset, headset, and speakerphone volume (off hook) and the ringer volume (on hook).
14	Messages button 	Autodials your voice messaging system (varies by system).
15	Applications button 	Opens or closes the Applications menu. Use the Applications button to access call history, user preferences, phone settings, and phone model information.
16	Contacts button 	Opens or closes the Directories menu. Use the Contacts button to access personal and corporate directories.
17	Handset	Phone handset.

## Terminology differences

The following table highlights some of the differences in terminology found in the *Cisco IP Phone 7821, 7841, and 7861 User Guide for Cisco Unified Communications Manager (SIP)*, the *Cisco IP Phone 7821, 7841, and 7861 Administration Guide for Cisco Unified Communications Manager (SIP)*, and the *Cisco Unified Communications Administration Guide*.

**Table 6: Terminology differences**

User Guide	Administration Guides
Line Status	Busy Lamp Field (BLF)
Message Indicators	Message Waiting Indicator (MWI) or Message Waiting Lamp
Programmable Feature Button	Programmable Button or Programmable Line Key (PLK)

<b>User Guide</b>	<b>Administration Guides</b>
Voicemail System	Voice Messaging System



## PART **II**

# Cisco IP Phone Installation

- [Cisco IP Phone installation, page 31](#)
- [Cisco Unified Communications Manager phone setup, page 43](#)
- [Self Care Portal management, page 53](#)





# Cisco IP Phone installation

---

- [Verify network setup, page 31](#)
- [Enable autoregistration for phone , page 32](#)
- [Install Cisco IP Phone, page 33](#)
- [Set up phone from setup menus, page 35](#)
- [Configure network settings, page 37](#)
- [Verify phone startup, page 41](#)
- [Configure Phone Services for users, page 41](#)

## Verify network setup

When deploying a new IP telephony system, system administrators and network administrators must complete several initial configuration tasks to prepare the network for IP telephony service. For information and a checklist for setting up and configuring a Cisco IP telephony network, see the “System Configuration Overview” chapter in *Cisco Unified Communications Manager System Guide*.

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** (Optional) Configure a Voice over Wireless LAN (VoWLAN) to meet the following requirements:

- Cisco Aironet Access Points (APs) are configured to support VoWLAN.
  - Controllers and switches are configured to support VoWLAN.
  - Security is implemented for authenticating wireless voice devices and users.
- 

## Enable autoregistration for phone

The Cisco IP Phone requires Cisco Unified Communications Manager to handle call processing. See the *Cisco Unified Communications Manager Administration Guide* or the context-sensitive help in the Cisco Unified Communications Manager 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.

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

Autoregistration is disabled by default. In some cases, you might not want to use autoregistration; for example, if you want to assign a specific directory number to the phone, or if you want to use a secure connection with Cisco Unified Communications Manager as described in *Cisco Unified Communications Manager Security Guide*. For information about enabling autoregistration, see the “Enabling Autoregistration” section in the *Cisco Unified Communications Manager Administration Guide*. When you configure the cluster for mixed mode through the Cisco CTL client, autoregistration is automatically disabled. When you configure the cluster for nonsecure mode through the Cisco CTL client, autoregistration is not enabled automatically.

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 *Cisco Unified Communications Manager Administration Guide*.

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** Select the required server and then select the Autoregister check box.
- Step 3** Click **Save**.
- 

### Related Topics

[Phone addition methods, on page 48](#)

## Install Cisco IP Phone

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

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




---

**Note** Before using external devices, read [External devices, on page 13](#).

---

### Procedure

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

For more information, see [Phone power requirements, on page 6](#).

- Step 2** Connect the handset to the handset port.
- The wideband-capable handset is designed especially for use with a Cisco IP Phone. The handset includes a light strip that indicates incoming calls and waiting voice messages.

- Step 3** Connect a headset to the headset port. You can add a headset later if you do not connect one now. For more information, see [Headsets, on page 59](#).
- Step 4** Connect a wireless headset. You can add a wireless headset later if you do not want to connect one now. For more information, see your wireless headset documentation.
- Step 5** Connect a straight-through Ethernet cable from the switch to the network port labeled 10/100 SW on the Cisco IP Phone (10/100/1000 SW on Cisco IP Phone 7841). Each Cisco IP Phone ships with one Ethernet cable in the box. Use Category 3, 5, or 5e cabling for 10 Mbps connections; Category 5 or 5e for 100 Mbps connections; and Category 5e for 1000 Mbps connections. For more information, see [Network and computer port pinouts, on page 4](#).
- Step 6** Connect a straight-through Ethernet cable from another network device, such as a desktop computer, to the computer port on the Cisco IP Phone. You can connect another network device later if you do not connect one now.  
You can use Category 3, 5, or 5e cabling for 10 Mbps connections; Category 5 or 5e for 100 Mbps connections; and Category 5e for 1000 Mbps connections. For more information, see [Network and computer port pinouts, on page 4](#) for guidelines.
- Step 7** If the phone is on a desk, adjust the footstand. For more information, see [Connect footstand, on page 58](#).  
With a wall-mounted phone, you might need to adjust the handset rest to ensure that the receiver cannot slip out of the cradle. For more information, see [Adjust handset rest, on page 71](#)
- Step 8** 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.
- Step 9** If you are configuring the network settings on the phone, you can set up an IP address for the phone by either using DHCP or manually entering an IP address.  
See [Configure network settings, on page 37](#) and [Network setup, on page 157](#).
- Step 10** Upgrade the phone to the current firmware image.  
Firmware upgrades over the WLAN interface may take longer than upgrading over the wired interface, depending on the quality and bandwidth of the wireless connection. Some upgrades may take more than one hour.
- Step 11** Make calls with the Cisco IP Phone to verify that the phone and features work correctly.  
See the *Cisco IP Phone 7821, 7841, and 7861 User Guide for Cisco Unified Communications Manager (SIP)*.
- Step 12** Secure the phone with a cable lock. For more information, see [Secure the phone with cable lock, on page 59](#).
- Step 13** 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 IP Phones.
- 

### Related Topics

- [Cisco IP Phone hardware, on page 15](#)
- [Verify phone startup, on page 41](#)
- [Verify network setup, on page 31](#)

## Set up phone from setup menus

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

The phone includes the following setup menus:

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

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



### Note

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.

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

To display a configuration menu, follow these steps:


### Procedure

- 
- Step 1** Press **Applications** .
  - Step 2** Select **Admin Settings**.
  - Step 3** Select **Network Setup** or **Security Setup**.
 

**Note** For information about the Reset Settings menu, see [Maintenance](#), on page 189.
  - Step 4** Enter your user ID and password, if required, then click **Sign-In**.
  - Step 5** Perform one of these actions to display the desired menu:
    - Use the navigation arrows to select the desired menu and then press **Select**.

- Use the keypad on the phone to enter the number that corresponds to the menu.

**Step 6** To display a submenu, repeat step 5.

**Step 7** To exit a menu, press **Exit** or the back arrow .

---

## Apply 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 Admin Settings phone screen.

### Procedure

---

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


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

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

---

## Text and menu entry from phone

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

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



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

---

### Related Topics

[Apply phone password, on page 36](#)

[Basic reset, on page 189](#)

## Configure network settings

### Procedure

View and configure the following network settings:

- Domain name field
- Admin VLAN ID field
- PC VLAN field
- Software port configuration field
- PC port configuration field
- DHCP enabled field
- IP address field
- Subnet mask field
- Default router field
- DNS server field
- Alternate TFTP field
- TFTP server 1 and server 2 fields

### Related Topics

[Text and menu entry from phone, on page 36](#)

[Apply phone password, on page 36](#)

## Set Domain Name field

### Procedure

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

## Set Admin VLAN ID field

### Procedure

---

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

## Set PC VLAN field

### Procedure

---

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

## Set SW Port Configuration field

### Procedure

---

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

## Set PC Port Configuration field

### Procedure

---

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

## Set DHCP Enabled field

### Procedure

---

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

## Set IP Address field

### Procedure

---

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

## Set Subnet Mask field

### Procedure

---

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

## Set Default Router field

### Procedure

---

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

## Set DNS Server fields

### Procedure

---

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

## Set Alternate TFTP field

### Procedure

---

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

## Set TFTP Server 1 field

### Procedure

---

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



## Set TFTP Server 2 field

### Procedure

---

- Step 1** Unlock the CTL or ITL file if necessary (for example, if you are changing the administrative domain of the phone). If both the CTL and ITL files exist, unlock either of the files.
  - Step 2** Unlock network configuration options.
  - Step 3** Enter an IP address for the TFTP Server 1 option.
  - Step 4** Scroll to the TFTP Server 2 option, press **Select**, and enter a new backup TFTP server IP address. If there is no secondary TFTP Server, you can use **Delete** to clear the field of a previous value.
  - Step 5** Press **Apply** and then press **Save**.
- 

## Verify phone startup

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

### Procedure

---

- Step 1** If using Power over Ethernet, plug the LAN cable into the Network port.
  - Step 2** If using the power cube, connect the cube to the phone and plug the cube into an electrical outlet. The buttons flash amber and then green in sequence during the various stages of bootup as the phone checks the hardware.
- If the phone completes these stages successfully, it has started up properly and the **Select** button stays lit until it is selected.
- 

### Related Topics

[Startup problems, on page 171](#)

[Cisco IP Phone does not go through normal startup process, on page 171](#)

## 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 “Cisco Unified IP Phone Services Configuration” chapter in the *Cisco Unified Communications Manager Administration Guide* and the “Cisco Unified IP Phone Services” chapter in the *Cisco Unified Communications Manager System Guide*.

**Note**

---

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

---

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 53](#) for a summary of the information that you must provide to end users.
-



# Cisco Unified Communications Manager phone setup

---

- [Determine phone MAC address, page 43](#)
- [Set up Cisco IP Phone, page 43](#)
- [Phone addition methods, page 48](#)
- [Add users to Cisco Unified Communications Manager, page 49](#)
- [Add user to End User group, page 51](#)
- [Associate phones with users, page 51](#)

## Determine phone MAC address

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

### Procedure

Perform one of the following actions:

- On the phone, press **Applications > 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 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 Administration 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 *Cisco 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: see [Determine phone MAC address, on page 43](#)
- 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, softkey template, phone features, IP Phone services, or phone applications

For more information, see the “Cisco Unified IP Phones setup” chapter in the *Cisco Unified Communications Manager Administration Guide* and see [Telephony features for Cisco IP Phone, on page 90](#).

**Step 2** Verify that you have sufficient unit licenses for your phone.  
For more information, see the *Enterprise License Manager User Guide*.

**Step 3** Define the phone button templates that determine the configuration of buttons on a phone. Select **Device > Device Settings > Phone Button Template** to create and update the templates.  
For more information, see the “Phone button template setup” chapter in the *Cisco Unified Communications Manager Administration Guide* and [Phone button templates, on page 133](#).

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

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

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

For information about Product Specific Configuration fields, see the “?” Button Help in the Phone Configuration window.

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

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

**Note** Choose a security profile based on the overall security strategy of the company. If the phone does not support security, choose a nonsecure profile.
- d) In the Extension Information area, check the Enable Extension Mobility check box if this phone supports Cisco Extension Mobility.
- e) Click **Save**.

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

- a) Find the phone.
- b) In the Phone Configuration window, click Line 1 on the left pane of the window.
- c) In the Directory Number field, enter a valid number that can be dialed.
 

**Note** This field should contain the same number that appears in the Telephone Number field in the End User Configuration window.
- d) From the Route Partition drop-down list, choose the partition to which the directory number belongs. If you do not want to restrict access to the directory number, choose <None> for the partition.
- e) From the Calling Search Space drop-down list, choose the appropriate calling search space. The value that you choose applies to all devices that are using this directory number.

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

**Example:**

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

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

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

**Example:**

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

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

- h) Select **Save**.

For more information, see the “Directory number setup” chapter in the *Cisco Unified Communications Manager Administration Guide* and see [Telephony features for Cisco IP Phone](#), on page 90.

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

- a) Use **Find** in conjunction with the Search fields to locate the user.
- b) check the box next to the user name, and click **Add Selected**.  
The user name and user ID appears in the Users Associated With Line pane of the Directory Number Configuration window.
- c) Select **Save**.
- d) Select **Save**.  
The user is now associated with Line 1 on the phone.
- e) If the phone has a second line, configure Line 2.

**Step 11** Associate the user with the device:

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

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

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

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

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

For more information, see the “Softkey template setup” and “Cisco Unified IP Phone setup” chapters in the *Cisco Unified Communications Manager Administration Guide*.

**Step 13** Configure speed-dial buttons and assign speed-dial numbers. Select **Device > Phone**.

**Note** Users can change speed-dial settings on their phones using their Self Care Portal.

- a) Find the phone you want to set up.
- b) In the Association Information area, click **Add a new SD**.
- c) Set up the speed dial information.
- d) Select **Save**.

**Step 14** Configure Cisco IP Phone services and assign services. Select **Device > Device Settings > Phone Services**. Provides IP Phone services to the phone.

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

**Step 15** (Optional) Assign services to programmable buttons. Select **Device > Device Settings > Phone Button Profile**.

Provides access to an IP phone service or URL.

**Step 16** Add user information to the global directory for Cisco Unified Communications Manager. Select **User Management > End User** and configure the required fields. Required fields are indicated by an asterisk (\*); for example, User ID and last name.

**Note** If your company uses a Lightweight Directory Access Protocol (LDAP) directory to store information on users, you can install and configure Cisco Unified Communications to use your existing LDAP directory, see [Corporate Directory setup, on page 137](#). After the Enable Synchronization from the LDAP Server field is enabled, you will not be able to add additional users from Cisco Unified Communications Manager Administration.

**Note** If you want to add both the phone and user to the Cisco Unified Communications Manager database at the same time, see “End user phone addition” in *Cisco Unified Communications Manager Administration Guide*.

- a) Set the User ID and last name fields.
- b) Assign a password (for Self Care Portal).
- c) Assign a PIN (for Cisco Extension Mobility and Personal Directory).
- d) Associate the user with a phone.  
Provides users with control over their phone such a forwarding calls or adding speed-dial numbers or services.

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

**Step 17** Associate a user with a user group. Select **User Management > User Settings > Access Control Group**. Assigns users a common list of roles and permissions that apply to all users in a user group. Administrators can manage user groups, roles, and permissions to control the level of access (and, therefore, the level of security) for system users. For more information, see [Add user to End User group, on page 51](#).

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

For more information, see “End user setup” and “Access control group setup” in the *Cisco Unified Communications Manager Administration Guide*.

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

Adding phones individually or using BAT require you to identify the MAC address for the phone. For more information, see [Determine phone MAC address, on page 43](#).

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

### Related Topics

[Enable autoregistration for phone , on page 32](#)

## 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** and click **Add New**.
  - Step 2** Select the phone type.
  - Step 3** Select **Next**.
  - Step 4** If requested, select the Protocol and click **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 “Cisco Unified Communications Manager overview” chapter in the *Cisco Unified Communications Manager System Guide*.

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

---

## Add phones using BAT phone template

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

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

For detailed instructions about adding phones through the Bulk Administration menu, see the “Phone insertion” chapter of the *Cisco Unified Communications Manager Bulk Administration Guide*.

For more information about using BAT, see the *Cisco Unified Communications Manager Bulk Administration Guide*. For more information about creating of BAT Phone Templates, see the “Phone template” chapter in the *Cisco Unified Communications Manager Bulk Administration Guide*.

### 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** If required, select the device protocol and select **Next**.
  - Step 5** Enter the details of phone-specific parameters, such as Device Pool, Phone Button Template, Device Security Profile, and so on.
  - Step 6** Click **Save**.
  - Step 7** 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 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 user directly to Cisco Unified Communications Manager](#), on page 50.
- 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 “Cisco Unified Communications Manager Bulk Administration” chapter in the *Cisco Unified Communications Manager Administration Guide*.
- 

## Add user from external LDAP directory

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

### Procedure

---

- Step 1** Sign into Cisco Unified Communications Manager Administration.
- Step 2** Choose **System > LDAP > LDAP Directory**.
- Step 3** Use **Find** to locate your LDAP directory.
- Step 4** Click on the LDAP directory name.
- Step 5** Click **Perform Full Sync Now**.
- Note** If you do not need to synchronize the LDAP Directory to the Cisco Unified Communications Manager immediately, the LDAP Directory Synchronization Schedule on the LDAP Directory window determines when the next autosynchronization is scheduled. However, the synchronization must occur before you can associate a new user to a device.
- 

## Add user directly to Cisco Unified Communications Manager

If you are not using an LDAP directory, you can add a user directly with Cisco Unified Communications Manager Administration by following these steps:



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

---

### Procedure

---

- Step 1** Choose **User Management > End User**, then click **Add New**.
- Step 2** 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 3** Click **Save**.

---

## Add user to End User group

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

### Procedure

---

- Step 1** From Cisco Unified Communications Manager Administration, choose **User Management > User Groups**. The Find and List Users window displays.
  - Step 2** Enter the appropriate search criteria and click **Find**.
  - Step 3** Select the **Standard CCM End Users** link. The User Group Configuration window for the Standard CCM End Users appears.
  - Step 4** Select **Add End Users to Group**. The Find and List Users window appears.
  - Step 5** Use the Find User drop-down list boxes to find the users that you want to add and click **Find**. A list of users that matches your search criteria appears.
  - Step 6** In the list of records that appear, click the check box next to the users that you want to add to this user group. If the list is long, use the links at the bottom to see more results.
 

**Note** The list of search results does not display users that already belong to the user group.
  - Step 7** Choose **Add Selected**.
- 

## Associate phones with users

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

## Procedure

---

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



## Self Care Portal management

---

- [Self Care Portal overview, page 53](#)
- [Set up access to Self Care Portal, page 53](#)
- [Customize Self Care Portal display, page 54](#)

### Self Care Portal overview

From the Cisco Unified Communications Self Care Portal, users can customize and control phone features and settings. For information about the Self Care Portal, see the *Cisco Unified Communications Self Care Portal User Guide* located at [http://www.cisco.com/en/US/products/sw/voicesw/ps556/products\\_user\\_guide\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_user_guide_list.html).

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.

### Set up access to Self Care Portal

Use this procedure to enable a user to access the Self Care Portal.

#### Procedure

---

- Step 1** In the Cisco Unified Communications Manager Administration, select **User Management > End User**.
  - Step 2** Search for the user and click the user ID link.
  - Step 3** Ensure that the user has a password and PIN configured.
  - Step 4** Select **Save**.
-

## Customize Self Care Portal display

Most options that 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 the 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 IP Phone accessories, page 57](#)
- [Wall Mounts , page 63](#)







## Cisco IP Phone accessories

- [Cisco IP phone accessories overview, page 57](#)
- [Connect footstand, page 58](#)
- [Secure the phone with cable lock, page 59](#)
- [Headsets, page 59](#)

### Cisco IP phone accessories overview

The Cisco IP Phone 7821, 7841, and 7861 supports both Cisco and third-party accessories.

In the following table, an X indicates support for an accessory by a particular phone model and a dash (-) indicates no support.

**Table 7: Accessory support for the Cisco IP Phone 7821, 7841, and 7861**

Accessory	Type	Cisco IP Phone 7821	Cisco IP Phone 7841	Cisco IP Phone 7861
<b>Cisco Accessory</b>				
<b>Third-Party accessories</b>				
Headsets: See <a href="#">xref: Headsets</a> . This section includes information about each headset type.	Analog	X	X	X
	Analog Wideband	X	X	X
Microphone: See <a href="#">xref: External Speakers and Microphone</a> .	External PC	-	X	X
Speakers: See <a href="#">xref: External Speakers and Microphone</a> .	External PC	-	X	X

## 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.

---

## Secure the phone with cable lock

You can secure the phone to a desktop by using a laptop cable lock. The lock connects to the antitheft security connector on the back of the phone and the cable can be secured to a desktop.

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

### Procedure

- 
- Step 1** Wrap the looped end of the cable lock and wrap it around object to which you want to secure your phone.
- Step 2** Pass the lock through the looped end of the cable.
- Step 3** Unlock the cable lock.
- Note** There are two kinds of cable locks: keyed and combination. Depending on what type of lock you have, unlock it by using the key or the correct combination.
- Step 4** Press and hold the locking button to align the locking teeth.
- Step 5** Insert the cable lock into the lock slot of your phone and release the locking button.
- Step 6** Lock the cable lock.
- Note** For keyed locks, turn the key 90 degrees in the clockwise direction and pull the key out of the lock. For combination locks, rotate the lock 90 degrees and then scramble the combination.
- 

## Headsets

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

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

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




---

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

---

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

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

## Related Topics

[External devices](#), on page 13

## Audio quality

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

For additional information, see [http://www.cisco.com/en/US/partner/prod/voicesw/ucphone\\_headsets.html](http://www.cisco.com/en/US/partner/prod/voicesw/ucphone_headsets.html)

## Analog headsets

Analog headsets are supported on the Cisco IP Phone 7821, 7841, and 7861. However, the Cisco IP Phone 7821, 7841, and 7861 cannot detect when an analog headset is plugged in. For this reason, the analog headset displays by default in the Accessories window on the phone screen.

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


### Enable wideband on analog headsets

Although analog headsets are supported on the phone, the phones cannot detect when an analog headset is plugged in. For this reason, by default, the analog headset displays in the Accessories window on the phone screen.

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

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

#### Procedure

- 
- Step 1** On the Cisco IP Phone, press **Applications** .
  - Step 2** Select **Accessories**.
  - Step 3** Highlight the analog headset, then press **Setup**.
  - Step 4** Turn wideband on or off for the selected headset by using the on/off toggle.
- 

### Enable wideband codec on analog headsets

Although analog headsets are supported on the phone, the phones cannot detect when an analog headset is plugged in. For this reason, by default, the analog headset displays in the Accessories window on the phone screen.

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

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

### Procedure

---

- Step 1** In Cisco Unified Communications Manager Administration, choose **Device > Phone**.
  - Step 2** In the Find and List Phones window, enter the search criteria for the phone to which you want to add the analog headset, then click **Find**.
  - Step 3** Click on the Device Name that you want. The Phone Configuration window displays.
  - Step 4** On the Product Specific Configuration Layout portion of the Phone Configuration window, ensure that the Wideband Headset UI Control option is enabled. (This option is enabled by default.)
  - Step 5** In the Product Specific Configuration Layout portion of the Phone Configuration window, you can also set the Wideband Headset option. (This option is also enabled by default).
- 

## Wired headsets

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

### 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 wired headset

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

#### Procedure

---

- Step 1** To disable the headset from Cisco Unified Communications Manager Administration, choose **Device > Phone** and locate the phone that you want to modify.
  - Step 2** In the Phone Configuration window (Product Specific Configuration layout portion), select the **Disable Speakerphone and Headset** check box.
-





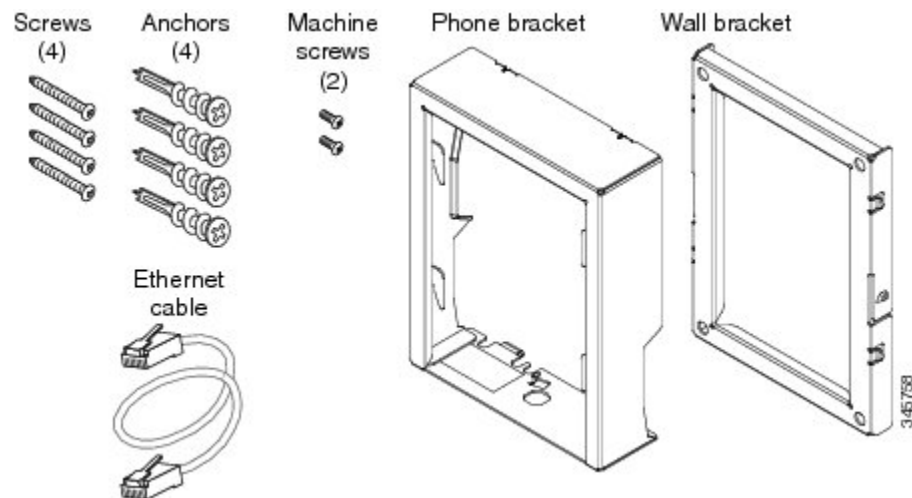
## Wall Mounts

- [Non-lockable wall mount components, page 63](#)
- [Adjust handset rest, page 71](#)

### Non-lockable wall mount components

The following figure shows the contents of the Wall Mount kit.

**Figure 1: Components**



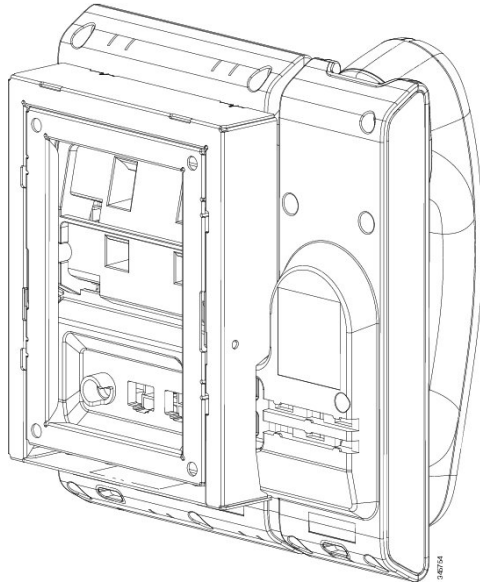
The package includes these items:

- One phone bracket
- One wall bracket
- Four #8-18 x 1.25-inch Phillips-head screws with four anchors
- Two M2.5 x 6 mm machine screws
- One 6-inch Ethernet cable

This section describes how to install and remove the ADA non-lockable wall mount kit.

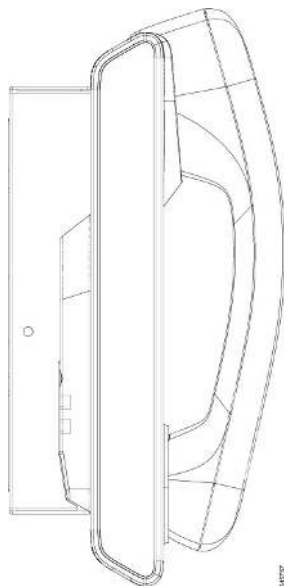
The following figure shows the wall mount kit installed on the phone.

**Figure 2: Back view of ADA non-lockable wall mount kit installed on phone**



The following figure shows the phone with the wall mount kit from the side.

**Figure 3: Side view of ADA non-lockable wall mount kit installed on phone**





## Install non-lockable wall mount kit

The wall mount kit can be mounted on most surfaces, including concrete, brick, and similar hard surfaces. To mount the kit on concrete, brick, or similar hard surfaces, you must provide the appropriate screws and anchors for your wall surface.

### Before You Begin

You need these tools to install the bracket:

- #1 and #2 Phillips-head screwdrivers
- Level
- Pencil

You must also install an Ethernet jack for the telephone in the desired location if an Ethernet jack does not currently exist. This jack must be wired appropriately for an Ethernet connection. You cannot use a regular telephone jack.

### Procedure

---

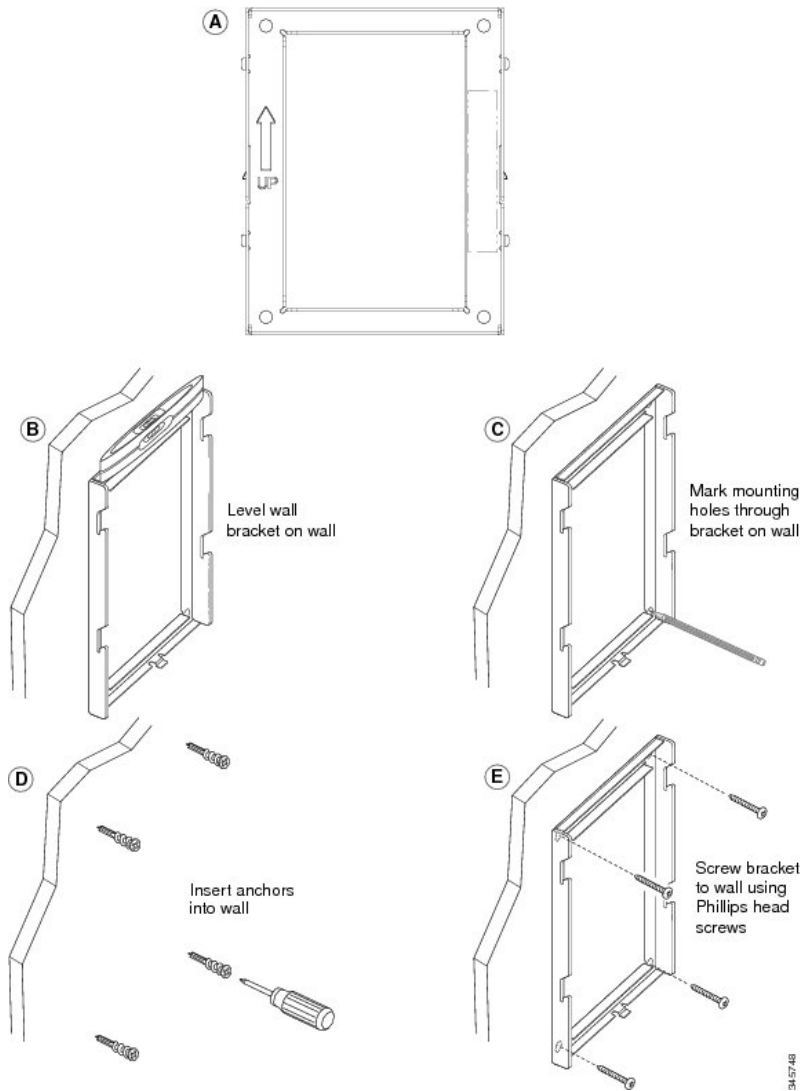
**Step 1** Mount the wall bracket in the desired location. You can install the bracket over an Ethernet jack, or you can run the Ethernet network cable to a nearby jack.

**Note** If the jack is to be placed behind the phone, the Ethernet jack must be flush to the wall or recessed.

- a) Hold the bracket on the wall, placing it so that the arrow on the back of the bracket is pointing up.
- b) Use the level to ensure that the bracket is level and use a pencil to mark the screw holes.
- c) Using a #2 Phillips-head screwdriver, carefully center the anchor over the pencil mark and press the anchor into the wall.
- d) Screw the anchor clockwise into the wall until it is seated flush.
- e) Use the included screws and a #2 Phillips-head screwdriver to attach the bracket to the wall.

The following figure shows the bracket installation steps.

**Figure 4: Bracket installation**

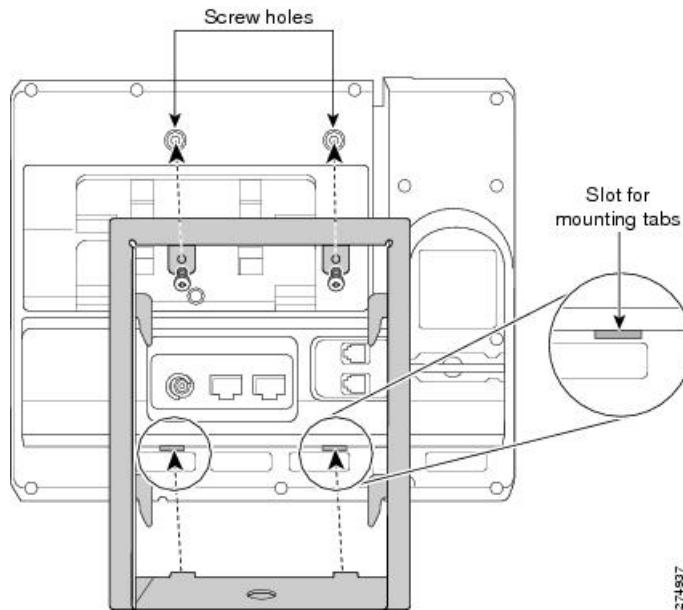


**Step 2** Attach the phone bracket to the IP Phone.

- Detach the handset cord (and headset cord, if there is a headset), power cord, and any other attached cords from the base of the phone.
- Remove the label covers that conceal the screw holes.
- Attach the phone bracket by inserting the tabs into the mounting tabs on the back of the phone. The phone ports should be accessible through the holes in the bracket.
- Secure the phone bracket to the IP phone with the machine screws, using the #1 Phillips-head screwdriver.
- Thread the handset cord (and headset cord, if using one). Reattach the cords and seat them in the clips that are incorporated into the phone body.

The following figure shows how the bracket attaches to the phone.

**Figure 5: Attach phone bracket**

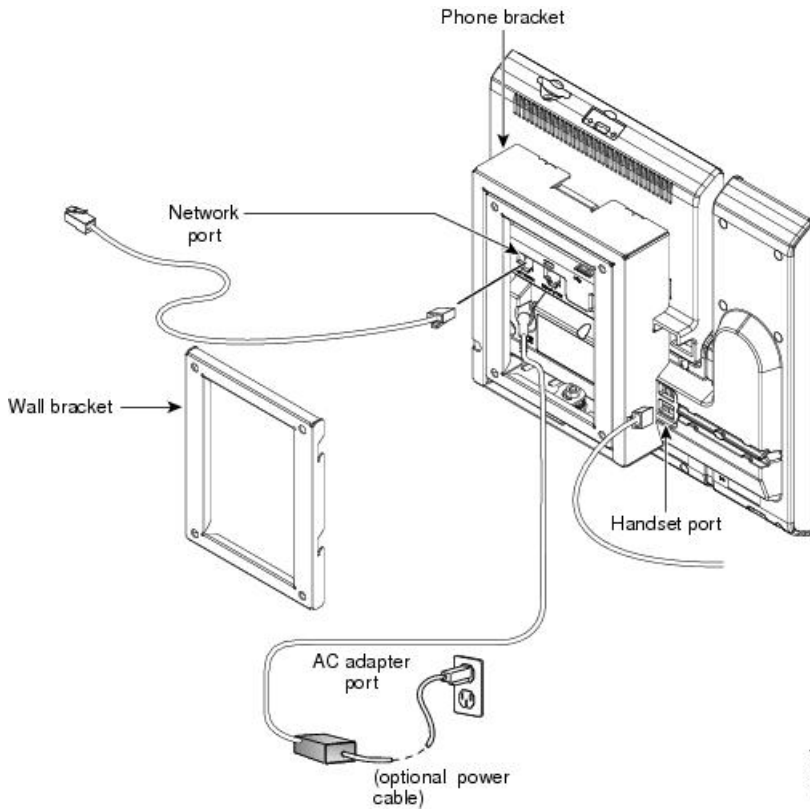


**Step 3** Attach the cables to the phone:

- a) Attach the Ethernet cable to the 10/100/1000 SW network port and wall jack.
- b) (Optional) If you are connecting a network device (such as a computer) to the phone, attach the cable to the 10/100/1000 Computer (PC access) port.
- c) (Optional) If you are using an external power supply, plug the power cord into the phone and dress the cord by clipping it into the clips that are incorporated into the phone body next to the PC port.
- d) (Optional) If the cables terminate inside the wall bracket, connect the cables to the jacks.

The following figure shows the cables.

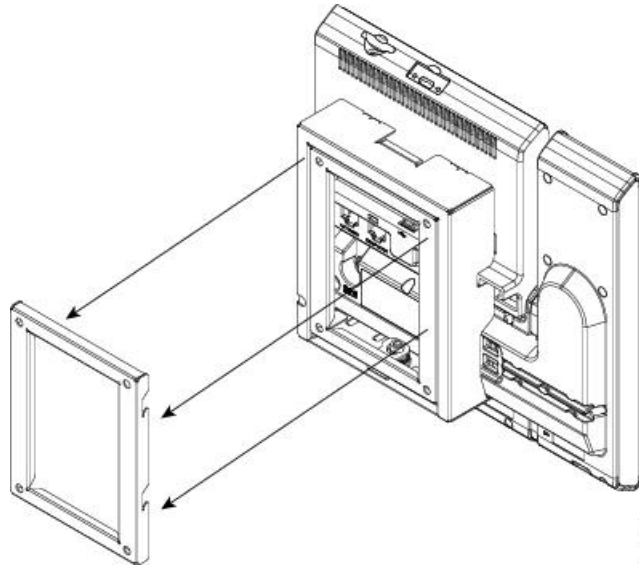
**Figure 6: Attach cables**



- Step 4** Attach the phone to the wall bracket by inserting the tabs on the top of the phone bracket into the slots on the wall bracket.  
 For cables that terminate outside of the brackets, use the cable-access openings in the bottom of the bracket to position the power cord and any other cable that does not terminate in the wall behind the bracket. The phone and wall bracket openings together form circular openings with room for one cable per opening.

The following figure shows how you attach the phone to the wall bracket.

**Figure 7: Attach phone to wall bracket**

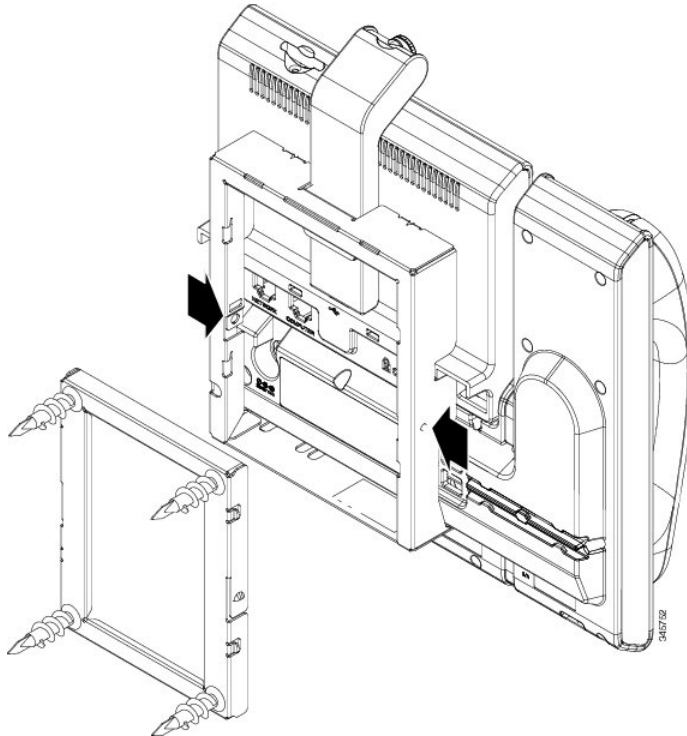


- Step 5** Press the phone firmly into the wall bracket and slide the phone down. The tabs in the bracket click into position.
- Step 6** Proceed to [Adjust handset rest](#), on page 71.
-

## Remove phone from non-lockable wall mount

The phone mounting plate contains two tabs to lock the plate into the wall bracket. The following figure shows the location and shape of the tabs.

**Figure 8: Tab location**



To remove the phone and mounting plate from the wall bracket, you must disengage these tabs.

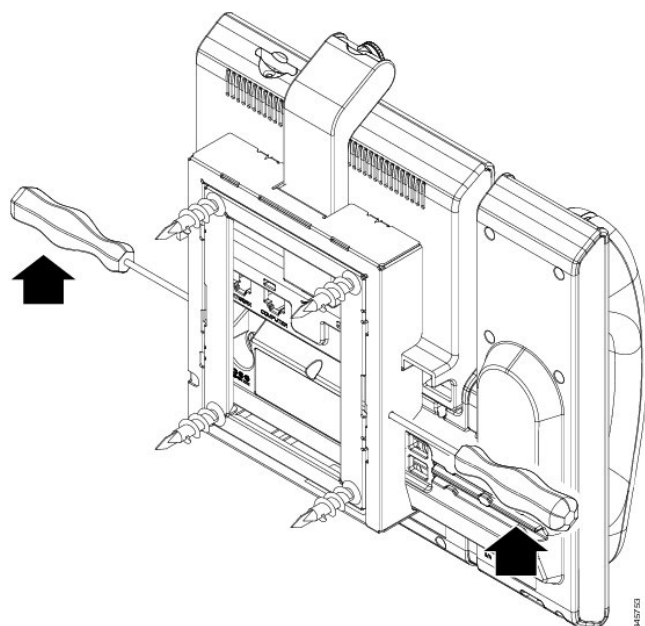
### Before You Begin

You require 2 screwdrivers or metal rods.

## Procedure

- Step 1** Push the screw drivers into the left and right holes in the phone mounting plate approximately 1 in. (2.5 cm).
- Step 2** Lift the screwdriver handles up to put a downward pressure on the tabs.

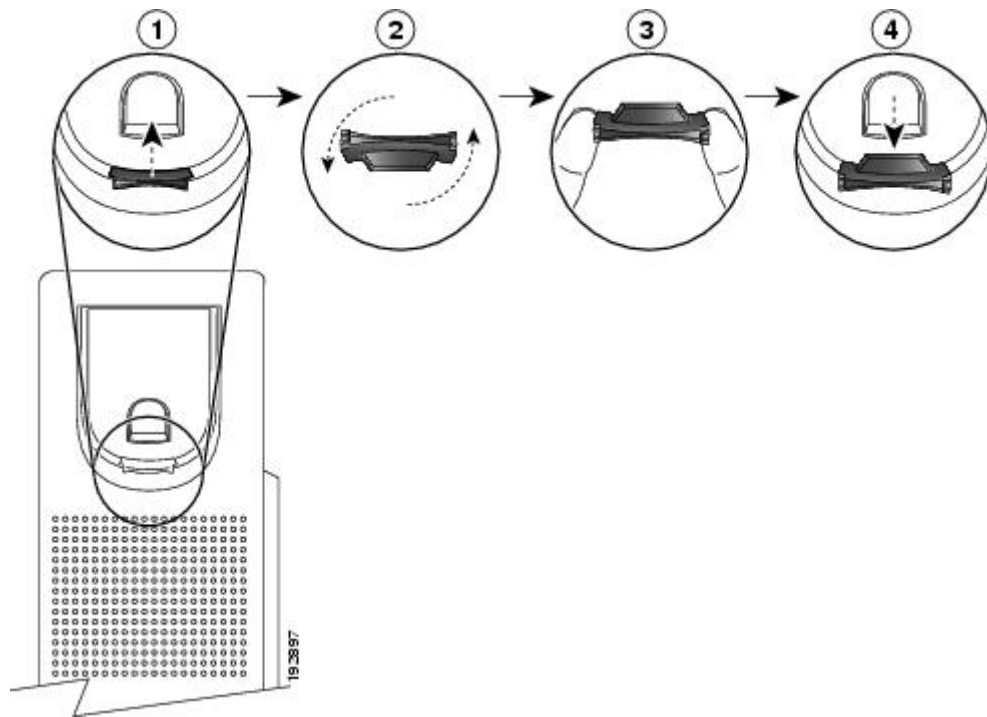
**Figure 9: Disengage tabs**



- Step 3** Press firmly to disengage the tabs and lift the phone at the same time to release the phone from the wall bracket.

## Adjust handset rest

If your phone is wall-mounted, you may need to adjust the handset rest to ensure that the receiver does not slip out of the cradle.



### Procedure

- 
- Step 1** Remove the handset from the cradle and pull the plastic tab from the handset rest.
  - Step 2** Rotate the tab 180 degrees.
  - Step 3** Hold the tab between two fingers, with the corner notches facing you.
  - Step 4** Line up the tab with the slot in the cradle and press the tab evenly into the slot. An extension protrudes from the top of the rotated tab.
  - Step 5** Return the handset to the handset rest.
-





# PART **IV**

## **Cisco IP Phone Administration**

- [Cisco IP Phone security, page 75](#)
- [Cisco IP Phone customization, page 85](#)
- [Phone Features and Setup , page 89](#)
- [Corporate and Personal Directory setup, page 137](#)





## Cisco IP Phone security

---

- [Cisco IP phone security overview, page 75](#)
- [View current security features on phone, page 76](#)
- [View Security Profiles, page 76](#)
- [Supported security features, page 76](#)

### Cisco IP phone security overview

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

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

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

**Note**

---

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

---

For more information about the security features, see the *Cisco Unified Communications Manager Security Guide*.

A Locally Significant Certificate (LSC) installs on phones after you perform the necessary tasks that are associated with the Certificate Authority Proxy Function (CAPF). You can use Cisco Unified Communications Manager Administration to configure an LSC, as described in the *Cisco Unified Communications Manager Security Guide*.

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

## View current security features on phone

View the security features of the Cisco IP Phone 7821, 7841, and 7861.

For more information about these features and about Cisco Unified Communications Manager and Cisco IP Phone security, see *Cisco Unified Communications Manager Security Guide*.

### Procedure

---

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

**Step 2** Select **Admin Settings > Security Setup**.

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*.

---

## 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 *Cisco Unified Communications Manager Security Guide*.

### Procedure

Look at the Security Mode setting in the Security Configuration menu.

## Supported security features

The following table provides an overview of the security features that the Cisco IP Phone 7821, 7841, and 7861 support. For more information about these features and about Cisco Unified Communications Manager and Cisco IP Phone security, see *Cisco Unified Communications Manager Security Guide*.

**Table 8: 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.

Feature	Description
Customer-site certificate installation	Each Cisco 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.
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 will not register phones unless they can be 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. 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 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 <code>cnf.xml</code> file and sends the file to the phone. A secure phone then uses a TLS connection to interact with the SRST-enabled router.
Media encryption	Uses SRTP to ensure that the media streams between supported devices proves secure and that only the intended device receives and reads the data. Includes creating a media master key pair for the devices, delivering the keys to the devices, and securing the delivery of the keys while the keys are in transport.
CAPF (Certificate Authority Proxy Function)	Implements parts of the certificate generation procedure that are too processing-intensive for the phone, and interacts with the phone for key generation and certificate installation. The CAPF can be configured to request certificates from customer-specified certificate authorities on behalf of the phone, or it can be configured to generate certificates locally.
Security profiles	Defines whether the phone is nonsecure or encrypted.
Encrypted configuration files	Lets you ensure the privacy of phone configuration files.

Feature	Description
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.
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 IP Phone can use 802.1X authentication to request and gain access to the network.

### Related Topics

[Cisco IP Phone security, on page 75](#)

[802.1X authentication, on page 82](#)

[View Security Profiles, on page 76](#)

## Set up Locally Significant Certificate

Use this procedure to configure an LSC on the phone.

### Before You Begin

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

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

For more information about these settings, see the “Configuring the Cisco CTL Client” section in 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, press **Applications** and choose **Admin Settings > Security Setup**.

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

**Step 3** Choose **LSC** and press **Select** or **Update**.

The phone prompts for an authentication string.

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

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


The LSC install, update, or removal process can take a long time to complete. You can stop the process at any time by pressing the **Stop** softkey from the Security Setup menu.

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

## 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 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 Conference Call Identification

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

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



#### Note

Interactions, restrictions, and limitations that affect the security level of the conference call depend on the security mode of the participant phones and the availability of secure conference bridges.

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

**Table 9: Security restrictions with conference calls**


Initiator phone security level	Feature used	Security level of participants	Results of action
Nonsecure	Conference	Secure	Nonsecure conference bridge Nonsecure conference
Secure	Conference	At least one member is nonsecure.	Secure conference bridge Nonsecure conference
Secure	Conference	Secure	Secure conference bridge Secure encrypted level conference
Nonsecure	Meet Me	Minimum security level is encrypted.	Initiator receives message Does not meet Security Level, call rejected.
Secure	Meet Me	Minimum security level is nonsecure.	Secure conference bridge Conference accepts all calls.



## Secure Phone Call Identification

A secure call is established when your phone, and the phone on the other end, is configured for secure calling. The other phone can be in the same Cisco IP network, or on a network outside the IP network. Secured calls can only be made between two phones. Conference calls and other multiple-line calls are not supported.

A secured call is established using this process:

- 1 A user initiates the call from a secured phone (secured security mode).
- 2 The phone displays the secure icon  on the phone screen. This icon indicates that the phone is configured for secure calls, but this does not mean that the other connected phone is also secured.
- 3 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

Secured calling is supported for conversations between two phones. Some features, such as conference calling and shared lines, are not available when secured 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 accordingly. At that time, 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 for connections between two phones only. Some features, such as conference calling, shared lines, and Extension Mobility, are not available when secure calling is configured.

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

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.
- **Enter MD5 Shared Secret:** If you disable 802.1X authentication or perform a factory reset on the phone, the previously configured MD5 shared secret is deleted.





## Cisco IP Phone customization

---

- [Custom phone rings, page 85](#)
- [Set up wideband codec, page 87](#)
- [Set up idle display, page 88](#)

### Custom phone rings

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



---

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

---

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

### Set Up Custom Phone Ring

To create custom phone rings for the Cisco 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 86](#).
- Step 2** Upload the new PCM files that you created to the Cisco TFTP server for each Cisco Unified Communications Manager in your cluster. For more information, see the “Software Upgrades” chapter in *Cisco Unified Communications Operating System Administration Guide*.
- Step 3** Use a text editor to edit the Ringlist.xml file. See [Custom ring file formats, on page 86](#) for information about how to format this file and for a sample Ringlist.xml file.
- Step 4** Save your modifications and close the Ringlist.xml file.
- Step 5** To cache the new Ringlist.xml file, stop and start the TFTP service by using Cisco Unified Serviceability or disable and reenable the “Enable Caching of Constant and Bin Files at Startup” TFTP service parameter, located in the Advanced Service Parameters area.
- 

## Custom ring file formats

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

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

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

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

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



### Note

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

This example shows a Ringlist.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.

## Set up wideband codec

By default, the G.722 codec is enabled for the Cisco IP Phone 7821, 7841, and 7861. If Cisco Unified Communications Manager is configured to use G.722 and if the far endpoint supports G.722, the call connects using the G.722 codec in place of G.711.

This situation occurs regardless of whether the user has enabled a wideband headset or wideband handset, but if either the headset or handset is enabled, the user may notice greater audio sensitivity during the call. Greater sensitivity means improved audio clarity but also means that the far endpoint can hear more background noise: noise such as rustling papers or nearby conversations. Even without a wideband headset or handset, some users may prefer the additional sensitivity of G.722 distracting. Other users may prefer the additional sensitivity of G.722.

The Advertise G.722 Codec service parameter affects whether wideband support exists for all devices that register with this Cisco Unified Communications Manager server or for a specific phone, depending on the Cisco Unified Communications Manager Administration window where the parameter is configured:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	To enable wideband support for all phones, perform the following steps:	
<b>Step 2</b>	To enable wideband support for a specific phone, perform the following steps:	

## 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 Unified 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 *Cisco Unified Communications Manager Administration Guide* or the *Cisco Unified Communications Manager Bulk Administration Guide* for the following information:

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

### Procedure

---

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





# CHAPTER 10

## Phone Features and Setup

---

- [Cisco IP Phone user support, page 90](#)
- [Telephony features for Cisco IP Phone, page 90](#)
- [Feature buttons and softkeys, page 107](#)
- [Create Feature Control Policy, page 109](#)
- [Disable speakerphone, page 111](#)
- [Schedule Power Save for Cisco IP Phone, page 111](#)
- [Schedule Power Save Plus \(EnergyWise\) on Cisco IP Phone, page 112](#)
- [Enable Agent Greeting, page 115](#)
- [Set up Do Not Disturb, page 116](#)
- [Set up monitoring and recording, page 117](#)
- [Set up Power Negotiation for LLDP, page 117](#)
- [Set up cBarge, page 118](#)
- [Set up Automatic Port Synchronization, page 118](#)
- [Set up SSH Access, page 119](#)
- [Set up Call Forward Notification, page 119](#)
- [Set up Client Matter Codes, page 120](#)
- [Enable Line Status for Call Lists, page 121](#)
- [Set up Forced Authorization Codes, page 121](#)
- [Set up Incoming Call Toast Timer, page 122](#)
- [Set up Peer Firmware Sharing, page 122](#)
- [Set up Remote Port Configuration, page 123](#)
- [Enable Device Invoked Recording, page 124](#)
- [Set Headset Sidetone Control, page 124](#)
- [Enable Actionable Incoming Call Alert, page 125](#)

- [Enable Call History for Shared Line](#), page 126
- [Control phone web page access](#), page 126
- [UCR 2008 setup](#), page 127
- [Set up softkey template](#), page 129
- [Set minimum ring volume](#), page 132
- [Set up Join and Direct Transfer Policy](#), page 132
- [Set up HTTPS for Phone Services](#), page 133
- [Phone button templates](#), page 133

## 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 Speed Dial, Services, and voice message system options), users must receive information from you or from your network team or must be able to contact you for assistance. Make sure to provide users with the names of people to contact for assistance and with instructions for contacting those people.

Cisco recommends 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 for Cisco IP Phone

After you add Cisco IP Phones to Cisco Unified Communications Manager, you can add functionality to the phones. The following table includes a list of supported telephony features, many of which you can configure by using Cisco Unified Communications Manager Administration.

For information about using most of these features on the phone, see *Cisco IP Phone 7821, 7841, and 7861 User Guide for Cisco Unified Communications Manager*. See [Feature buttons and softkeys](#), on page 107 for a list of features that can be configured as programmable buttons and dedicated softkeys and feature buttons.

**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*.

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.

Feature	Description and more information
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. 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 setup”</li> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phone”</li> </ul>
Agent Greeting	<p>Allows an agent to create and update a prerecorded greeting that plays at the beginning of 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 115.</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	<p>Enables users to park a call by pressing only one button using the Direct Park feature. Administrators must configure a Busy Lamp Field (BLF) Assisted Directed Call Park button. When users press an idle BLF Assisted Directed Call Park button for an active call, the active call is parked at the Direct Park slot associated with the Assisted Directed Call Park button.</p> <p>See the <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Assisted Directed Call Park” chapter.</p>
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. You hear 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>

Feature	Description and more information
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>Synchronizes ports to the lowest speed between ports of a phone to eliminate packet loss.</p> <p>See <a href="#">Set up Automatic Port Synchronization</a>, on page 118.</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>
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>
Busy Lamp Field (BLF)	<p>Allows a user to monitor the call state of a directory number associated with a speed-dial button on the phone.</p> <p>See the <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Presence” chapter.</p>
Busy Lamp Field (BLF) Pickup	<p>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.</p> <p>See the <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Call Pickup” chapter.</p>
Call Back	<p>Provides users with an audio and visual alert on the phone when a busy or unavailable party becomes available.</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>, “Cisco Call Back”</li> </ul>

Feature	Description and more information
Call Display Restrictions	<p>Determines the information that will display for calling or connected lines, depending on the parties who are involved in the call.</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> </ul>
Call Forward	<p>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.</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> <li>• <a href="#">Customize Self Care Portal display, on page 54</a></li> </ul>
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>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 Configurable Display	<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:</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>

Feature	Description and more information
Call Forward Notification	Allows you to configure the information that the user sees when receiving a forwarded call. See <a href="#">Set up Call Forward Notification</a> , on page 119.
Call History for Shared Line	Allows you to view shared line activity in the phone Call History. This feature will: <ul style="list-style-type: none"> <li>• Log missed calls for a shared line</li> <li>• Log all answered and placed calls for a shared line</li> </ul> See <a href="#">Enable Call History for Shared Line</a> , on page 126
Call Park	Allows users to park (temporarily store) a call and then retrieve the call by using another phone in the Cisco Unified Communications Manager system. See the <i>Cisco Unified Communications Manager Features and Services Guide</i> , “Call Park and Directed Call Park” chapter.
Call Pickup	Allows users to redirect a call that is ringing on another phone within their pickup group to their phone. You can configure an audio and visual alert for the primary line on the phone. This alert notifies the users that a call is ringing in their pickup group. See the <i>Cisco Unified Communications Manager Features and Services Guide</i> , “Call Pickup” chapter.
Call Recording	Allows a supervisor to record an active call. The user might hear a recording audible alert tone during a call when it is being recorded. When a call is secured, the security status of the call is displayed as a lock icon on Cisco IP Phones. The connected parties might also hear an audible alert tone that indicates the call is secured and is being recorded. <b>Note</b> When an active call is being monitored or recorded, the user can receive or place intercom calls; however, if the user places an intercom call, the active call is put on hold, 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. See the <i>Cisco Unified Communications Manager Features and Services Guide</i> , “Monitoring and Recording” chapter.
Call Waiting	Indicates (and allows users to answer) an incoming call that rings while on another call. Incoming call information appears on the phone display. See the <i>Cisco Unified Communications Manager System Guide</i> , “Understanding Directory Numbers”.
Call Waiting Ring	Provides Call Waiting users with the option of an audible ring instead of the standard beep. Options are Ring and Ring Once. See the <i>Cisco Unified Communications Manager System Guide</i> , “Directory Numbers”.

Feature	Description and more information
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>
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 the <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Calling Party Normalization” chapter.</p>
CAST for SIP	<p>Establishes communication between the Cisco Unified Video Advantage (CUVA) and the Cisco IP phones to support video on the PC even if the IP phone does not have video capability.</p> <p>See the <i>Cisco Unified Communications Manager Features and Services Guide</i>.</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>

Feature	Description and more information
Cisco Extension Mobility	<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>See the <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Cisco Extension Mobility” chapter.</p>
Cisco Extension Mobility Cross Cluster (EMCC)	<p>Enables a user configured in one cluster to log into a Cisco IP Phone in another cluster. Users from a home cluster log into a Cisco IP Phone at a visiting cluster.</p> <p><b>Note</b> Configure Cisco Extension Mobility on Cisco 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>
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, on page 12</a></li> </ul>
Cisco Unified Video Advantage (CUVA)	<p>Allows users to make video calls by using a Cisco IP Phone, a personal computer, and an external video camera.</p> <p><b>Note</b> Configure the Video Capabilities parameter in the Product Specific Configuration Layout section in Phone Configuration.</p> <p>See the Cisco Unified Video Advantage documentation.</p>
Cisco WebDialer	<p>Allows users to make calls from web and desktop applications.</p> <p>See the <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Cisco WebDialer” chapter.</p>
Classic Ringtone	<p>Supports 29 ringtones: 2 embedded in the phone firmware and 27 downloaded from the Cisco Unified Communications Manager. The feature makes the available ringtones common with other Cisco IP Phones.</p> <p>See <a href="#">Custom phone rings, on page 85</a>.</p>
Client Matter Code (CMC)	<p>Enables a user to specify that a call relates to a specific client matter.</p> <p>See <a href="#">Set up Client Matter Codes, on page 120</a>.</p>



Feature	Description and more information
Conference	<p>Allows a user to talk simultaneously with multiple parties by calling each participant individually. Conference features include Conference and Meet Me.</p> <p>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>The Advance Adhoc Conference service parameter, disabled by default in Cisco Unified Communications Manager Administration, allows you to enable these features.</p> <p>See the <i>Cisco Unified Communications Manager System Guide</i>, “Conference Bridges” and “Cisco Unified IP Phone” chapters.</p> <p><b>Note</b> Be sure to inform your users whether these features are activated.</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>
Debug Phone	<p>Provides an additional menu on the phone for debugging phone problems.</p> <p>See <a href="#">Troubleshoot using Debug menu, on page 187</a>.</p>
Device Invoked Recording	<p>Provides end users with the ability to record their telephone calls via a softkey.</p> <p>In addition administrators may continue to record telephone calls via the CTI User Interface.</p> <p>See <a href="#">Enable Device Invoked Recording, on page 124</a>.</p>
Direct Transfer	<p>Allows users to connect two calls to each other without remaining on the line.</p> <p>See the <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phone” chapter.</p>
Directed Call Park	<p>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.</p> <p><b>Note</b> If you implement Directed Call Park, avoid configuring the Park softkey. This prevents users from confusing the two Call Park features.</p> <p>See the <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Call Park and Directed Call Park” chapter.</p>
Disable Single Button Barge	<p>The softkeys are controlled by configuration in the Cisco Unified Communications Manager. The Line Key Barge parameter in the Administration window has the following options:</p> <ul style="list-style-type: none"> <li>• Default: The Barge and cBarge buttons are always available for use by the user.</li> <li>• Off: The Barge and cBarge buttons are never available by use by the user</li> <li>• Turn on softkey: The Barge and cBarge buttons are displayed, if configured in the phone profile.</li> </ul> <p>See the <i>Cisco Unified Communications Manager Administration Guide</i>.</p>

Feature	Description and more information
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.
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.
Divert	Allows a user to transfer a ringing, connected, or held call directly to a voice-messaging system. When a call is diverted, the line becomes available to make or receive new calls. See the <i>Cisco Unified Communications Manager Features and Services Guide</i> , “Immediate Divert” chapter.
Do Not Disturb (DND)	When DND is turned on, either no audible rings occur during the ringing-in state of a call, or no audible or visual notifications of any type occur. See <a href="#">Set up Do Not Disturb</a> , on page 116.
EnergyWise	Enables an IP Phone to sleep (power down) and wake (power up) at predetermined times, to promote energy savings. See <a href="#">Schedule Power Save Plus (EnergyWise) on Cisco IP Phone</a> , on page 112.
Enhanced Secure Extension Mobility Cross Cluster (EMCC)	Improves the Secure Extension Mobility Cross Cluster (EMCC) feature by preserving the network and security configurations on the login phone. By so doing, security policies are maintained, network bandwidth is preserved and network failure is avoided within the visiting cluster (VC). See the <i>Cisco Unified Communications Manager Features and Services Guide</i> , “Cisco Extension Mobility Cross Cluster” chapter.
Fast Dial Service	Allows a user to enter a Fast Dial code to place a call. Fast Dial codes can be assigned to phone numbers or Personal Address Book entries. See “Services” in this table. See <a href="#">Modify phone button template for PAB or Fast Dial</a> , on page 135.
Forced Authorization Code (FAC)	Controls the types of calls that certain users can place. See <a href="#">Set up Forced Authorization Codes</a> , on page 121.
Headset Sidetone Control	Allows an administrator to set the sidetone level of a wired headset. See <a href="#">Set Headset Sidetone Control</a> , on page 124.
Group Call Pickup	Allows a user to answer a call that is ringing on a directory number in another group. See the <i>Cisco Unified Communications Manager Features and Services Guide</i> , “Call Pickup” chapter.

Feature	Description and more information
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 not resumed.</p> <p>A call that triggers Hold Reversion also displays an animated icon in the call bubble. 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>
Hold/Resume	<p>Allows the user to move a connected call from an active state to a held state.</p> <ul style="list-style-type: none"> <li>• No configuration required unless you want to use Music On Hold. See “Music On Hold” in this table for information.</li> <li>• See “Hold Reversion” in this table.</li> </ul>
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>
HTTPS for Phone Services	<p>Increases security by requiring communication using HTTPS.</p> <p><b>Note</b> IP Phones can be HTTPS clients; they cannot be HTTPS servers.</p> <p>See <a href="#">Set up HTTPS for Phone Services</a>, on page 133.</p>
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>
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 122.</p>

Feature	Description and more information
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>
Jitter Buffer	<p>The Jitter Buffer feature handles jitter from 10 milliseconds (ms) to 1000 ms for both audio and video streams.</p>
Join Across Lines	<p>Allows users to combine calls that are on multiple phone lines to create a conference call. Some JTAPI/TAPI applications are not compatible with the Join and Direct Transfer feature implementation on the Cisco IP Phone and you may need to configure the Join and Direct Transfer Policy to disable join and direct transfer on the same line or possibly across lines.</p> <p>See <a href="#">Set up Join and Direct Transfer Policy</a>, on page 132.</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>See <a href="#">Set up Join and Direct Transfer Policy</a>, on page 132.</p>
Log out of hunt groups	<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</a>, on page 129</li> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Understanding Route Plans”</li> </ul>
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. The Line Status states are</p> <ul style="list-style-type: none"> <li>• Unknown</li> <li>• Idle</li> <li>• Busy</li> <li>• DND</li> </ul> <p>See <a href="#">Enable Line Status for Call Lists</a>, on page 121.</p>

Feature	Description and more information
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>
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>
Message Waiting	<p>Defines directory numbers for message waiting on and off indicators. A directly-connected voice-message system uses the specified directory number to set or to clear a message waiting indication for a particular Cisco 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>See <a href="#">Set minimum ring volume, on page 132</a>.</p>
Missed Call Logging	<p>Allows a user to specify whether missed calls will be logged in the missed calls directory for a given line appearance.</p> <p>See the <i>Cisco Unified Communications Manager Administration Guide</i>, “Directory Number Configuration” chapter.</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>

Feature	Description and more information
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>
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 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, the user can receive or place intercom calls; however, if the user places 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>
Multilevel Precedence and Preemption (MLPP)	<p>Provides a method of prioritizing calls within your phone system. Use this feature when users work in an environment where they need to make and receive urgent or critical calls.</p> <p>See the <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Multilevel Precedence and Preemption” chapter.</p>
Multiple Calls Per Line Appearance	<p>Each line can support multiple calls. By default, the phone supports two active calls per line, and a maximum of six 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 maximum calls/busy trigger not more than 6/6. Any configuration more than 6/6 is not officially supported.</p> <p>See the <i>Cisco Unified Communications Manager Administration Guide</i>, “Directory Number Configuration” chapter.</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 handset or headset microphone.</p>
No Alert Name	<p>Makes it easier for end users to identify transferred calls by displaying the original caller's phone number. The call appears as an Alert Call followed by the caller's telephone number.</p>
Onhook 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>

Feature	Description and more information
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>
Phone Display Message for Extension Mobility Users	<p>This feature enhances the phone interface for the Extension Mobility user by providing friendly messages.</p>
PLK Support for Queue Statistics	<p>The PLK Support for Queue Statistics feature 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 129.</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>
Power Negotiation over LLDP	<p>Allows the phone to negotiate power using Link Level Endpoint Discovery Protocol (LLDP) and Cisco Discovery Protocol (CDP).</p> <p>See <a href="#">Set up Power Negotiation for LLDP</a>, on page 117.</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" chapter</li> <li>• <i>Cisco Unified Communications Manager System Guide</i>, "Cisco Unified IP Phone" chapter</li> <li>• <i>Cisco Unified Communications Manager Features and Services Guide</i>, "Barge and Privacy" chapter</li> </ul>
Private Line Automated Ringdown (PLAR)	<p>The Cisco Unified Communications Manager administrator can configure a phone number that the Cisco 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>
Programmable Feature Buttons	<p>You can 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>• <i>Cisco Unified Communications Manager System Guide</i>, "Cisco Unified IP Phone" chapter</li> <li>• <i>Cisco Unified Communications Manager Administration Guide</i>, "Phone Button Template Configuration" chapter</li> </ul>

Feature	Description and more information
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” chapter</li> <li>• <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Quality Report Tool” chapter</li> </ul>
Redial	<p>Allows users to call the most recently dialed phone number by pressing a button or the Redial softkey.</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 remote destination rings; desk phone does not ring. When the call is answered on their mobile phone, the desk phone displays a Remote In Use message. During these calls, users can make use of various features of their mobile phone.</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 123</a>.</p>
Ringtone 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” chapter</li> <li>• <a href="#">Custom phone rings, on page 85</a></li> </ul>
RTCP Hold For SIP	<p>Ensures that held calls are not dropped by the gateway. The gateway checks the status of the RTCP port to determine if a call is active or not. By keeping the phone port open, the gateway will not end held calls.</p>



Feature	Description and more information
Secure Conference	<p>Allows secure phones to place conference calls using a secured conference bridge. As new participants are added by using Confn, Join, cBarge, Barge softkeys or MeetMe 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 nonsecure 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="#">Supported security features, on page 76</a></li> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Conference Bridges” chapter</li> <li>• <i>Cisco Unified Communications Manager Administration Guide</i>, “Conference Bridge Configuration” chapter</li> <li>• <i>Cisco Unified Communications Manager Security Guide</i></li> </ul>
Secure EMCC	<p>Improves the EMCC feature by providing enhanced security for a user logging into their phone from a remote office.</p>
Services	<p>Allows you to use the Cisco 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” chapter</li> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phone Services” chapter</li> </ul>
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” chapter</li> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phone Services” chapter</li> </ul>
Show Calling ID and Calling Number	<p>The phones can display both the calling ID and calling number for incoming calls. The IP phone LCD display size limits the length of the calling ID and the calling number that display.</p> <p>The Show Calling ID and Calling Number feature applies to the incoming call alert only and does not change the function of the Call Forward and Hunt Group features.</p> <p>See “Caller ID” in this table.</p>

Feature	Description and more information
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>
SSH Access	<p>Allows you to enable or disable the SSH Access setting using Cisco Unified Communications Manager Administration. Enabling the SSH server allows the phone to accept the SSH connections. Disabling the SSH server functionality of the phone blocks the SSH access to the phone.</p> <p>See <a href="#">Set up SSH Access</a>, on page 119.</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 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 IP Phone and you may need to configure the Join and Direct Transfer Policy to disable join and direct transfer on the same line or possibly across lines.</p> <p>See <a href="#">Set up Join and Direct Transfer Policy</a>, on page 132.</p>
Transfer - Direct Transfer	<p>Transfer: The first invocation of Transfer will always initiate a new call by using the same directory number, after putting the active call on hold.</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 IP Phone and you may need to configure the Join and Direct Transfer Policy to disable join and direct transfer on the same line or possibly across lines.</p> <p>See:</p> <ul style="list-style-type: none"> <li>• <a href="#">Set up Join and Direct Transfer Policy</a>, on page 132</li> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Understanding Directory Numbers”</li> </ul>

Feature	Description and more information
TVS	<p>Trust Verification Services (TVS) enables phones to authenticate signed configurations and authenticate other servers or peers without increasing the size of the Certificate Trust List (CTL) or requiring the downloading of an updated CTL file to the phone. TVS is enabled by default.</p> <p>The Security Setting menu on the phone displays the TVS information.</p>
UCR 2008	<p>The Cisco IP Phones support Unified Capabilities Requirements (UCR) 2008 by providing the following functions:</p> <ul style="list-style-type: none"> <li>• Support for Federal Information Processing Standard (FIPS) 140-2</li> <li>• Support for 80-bit SRTCP Tagging</li> </ul> <p>As an IP Phone administrator, you must set up specific parameters in Cisco Unified Communications Manager Administration.</p> <p>See <a href="#">UCR 2008 setup, on page 127</a>.</p>
Voice Message 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” chapter</li> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Voice Mail Connectivity to Cisco Unified Communications Manager” chapter</li> </ul>
Web Access Disabled by Default	<p>Enhances security by disabling access to all web services, such as HTTP. Users can only access web services if you enable web access.</p> <p>See <a href="#">UCR 2008 setup, on page 127</a>.</p>

## Feature buttons and softkeys

The following table provides information about features that are available on softkeys, features that are available on dedicated feature buttons, and features that you need to configure as programmable feature buttons. An “X” in the table indicates that the feature is supported for the corresponding button type or softkey. Of the two button types and softkeys, only programmable feature buttons require configuration in Cisco IP Phone administration.

For information about configuring programmable feature buttons, see [Phone button templates, on page 133](#). For information about configuring features that can appear as softkeys or programmable buttons, see [Create Feature Control Policy, on page 109](#).

**Table 10: Features with corresponding buttons and softkeys**

Feature name	Dedicated feature button	Programmable feature button	Softkey
Alert Calls		X	
All Calls		X	
Answer		X	
Call Back		X	X
Call Forward All		X	X
Call Park		X	X
Call Park Line Status		X	
Call Pickup (Pick Up)		X	X
Call Pickup Line Status		X	
Conference	X		X (available while on a conference only)
Divert			X
Do Not Disturb		X	
Group Pickup (Group Pick Up)		X	X
Hold	X		
Hunt Groups		X	
Intercom		X	
Malicious Call Identification (MCID)		X	X
Meet Me		X	X
Mobile Connect (Mobility)		X	X
Mute	X		
Other Pickup		X	X

Feature name	Dedicated feature button	Programmable feature button	Softkey
PLK Support for Queue Status			X
Privacy		X	
Queue Status		X	
Quality Reporting Tool (QRT)		X	X
Redial		X	X
Speed Dial		X	X
Speed Dial Line Status		X	X
Transfer	X		X (available during a transfer only)

## Create Feature Control Policy

Feature Control Policies allow you to enable or disable a particular feature and thereby control the appearance of certain features and softkeys that display on the phone. You can configure multiple policies on Cisco Unified Communications Manager Administration. After you configure a Feature Control Policy, you must associate that policy to an individual phone, a group of phones, or to all phones in the system.

For more information, see the “Feature Control Policy” chapter in *Cisco Unified Communications Manager Administration Guide*.

### Procedure

- 
- Step 1** From Cisco Unified Communications Manager Administration, choose **Device > Device Settings > Feature Control Policy**.
- Step 2** Click **Add New** to define a set of policies.
- Step 3** Enter the following settings.
- Name: Enter a name for a new Feature Control Policy
  - Description: Enter a description.
  - Feature Control Section: Check the check box for the features for which you want to change the default setting.
- Step 4** Click **Save**.
- Step 5** Apply the policy to the phone by including it in the following windows:

- Enterprise Parameters Configuration: Applies to all phones in the system.
- Common Phone Profile Configuration: Applies to all phones in a group.
- Phone Configuration: Applies to an individual phone.

## Feature Control Policy default values

The following table lists the features that a Feature Control Policy can control and their default values.

**Table 11: Feature Control Policy default values**

Feature	Default value
Forward All	Enabled
Park	Disabled
To Voicemail	Disabled
Conference List	Enabled
Speed Dial	Enabled
Call Back	Enabled
Redial	Enabled
Barge	Enabled
Malicious Caller ID	Disabled
Pick Up	Disabled
Group Pick Up	Disabled
Other Pick Up	Disabled
Meet Me	Disabled
Quality Reporting Tool	Disabled
Mobility	Disabled

## 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.

### Procedure

---

- Step 1** 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**.
- 

## 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** From the Cisco Unified Communications Manager Administration, select **Device > Phone**.
- Step 2** Locate the phone that you need to set up.
- Step 3** Navigate to the Product Specific Configuration area and set the following fields.

Table 12: PowerSave configuration fields

Field	Description
Days Display Not Active	<p>Days that the display does not turn on automatically at the time specified in the Display On Time field.</p> <p>Choose the day or days from the drop-down list. To choose more than one day, Ctrl-click each day that you want.</p>
Display On Time	<p>Time each day that the display turns on automatically (except on the days specified in the Days Display Not Active field).</p> <p>Enter the time in this field in 24 hour format, where 0:00 is midnight.</p> <p>For example, to automatically turn the display on at 7:00 a.m., (0700), enter <b>7:00</b>. To turn the display on at 2:00 p.m. (1400), enter <b>14:00</b>.</p> <p>If this field is blank, the display will automatically turn on at 0:00.</p>
Display On Duration	<p>Length of time that the display remains on after turning on at the time specified in the Display On Time field.</p> <p>Enter the value in this field in the format <i>hours:minutes</i>.</p> <p>For example, to keep the display on for 4 hours and 30 minutes after it turns on automatically, enter <b>4:30</b>.</p> <p>If this field is blank, the phone will turn off at the end of the day (0:00).</p> <p><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.</p>
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>1:30</b>.</p> <p>The default value is 0:30.</p>

**Step 4** Select Save.

## Schedule Power Save Plus (EnergyWise) on Cisco IP Phone

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

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



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

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

### Procedure

- 
- Step 1** From the Cisco Unified Communications Manager Administration, select **Device > Phone**.
- Step 2** Locate the phone that you need to set up.
- Step 3** Navigate to the Product Specific Configuration area and set the following fields.

**Table 13: EnergyWise configuration fields**

Field	Description
Enable Power Save Plus	<p>Selects the schedule of days for which the phone powers off. Select multiple days by pressing and holding the Control key while clicking on the days for the schedule.</p> <p>By default, no days are selected.</p> <p>When Enable Power Save Plus is checked, you receive a message that warns about emergency (e911) concerns.</p> <p><b>Caution</b> While Power Save Plus Mode (the “Mode”) is in effect, endpoints that are configured for the mode are disabled for emergency calling and from receiving inbound calls. By selecting this mode, you agree to the following: (i) You take full responsibility for providing alternate methods for emergency calling and receiving calls while the mode is in effect; (ii) Cisco has no liability in connection with your selection of the mode and all liability in connection with enabling the mode is your responsibility; and (iii) You fully inform users of the effects of the mode on calls, calling and otherwise.</p> <p><b>Note</b> To disable Power Save Plus, you must uncheck the Allow EnergyWise Overrides check box. If the Allow EnergyWise Overrides remains checked but no days are selected in the Enable Power Save Plus field, Power Save Plus is not disabled.</p>
Phone On Time	<p>Determines when the phone automatically turns on for the days that are in the Enable Power Save Plus field.</p> <p>Enter the time in this field in 24-hour format, where 00:00 is midnight.</p> <p>For example, to automatically power up the phone at 7:00 a.m. (0700), enter 7:00. To power up the phone at 2:00 p.m. (1400), enter 14:00.</p> <p>The default value is blank, which means 00:00.</p> <p><b>Note</b> The Phone On Time must be at least 20 minutes later than the Phone Off Time. For example, if the Phone Off Time is 7:00, the Phone On Time must be no earlier than 7:20.</p>

Field	Description
Phone Off Time	<p>The time of day that the phone powers down for the days that are selected in the Enable Power Save Plus field. If the Phone On Time and the Phone Off Time fields contain the same value, the phone does not power down.</p> <p>Enter the time in this field in 24-hour format, where 00:00 is midnight.</p> <p>For example, to automatically power down the phone at 7:00 a.m. (0700), enter 7:00. To power down the phone at 2:00 p.m. (1400), enter 14:00.</p> <p>The default value is blank, which means 00:00.</p> <p><b>Note</b> The Phone On Time must be at least 20 minutes later than the Phone Off Time. For example, if the Phone Off Time is 7:00, the Phone On Time must be no earlier than 7:20.</p>
Phone Off Idle Timeout	<p>The length of time that the phone must be idle before the phone powers down.</p> <p>The timeout occurs under the following conditions:</p> <ul style="list-style-type: none"> <li>• When the phone was in Power Save Plus mode, as scheduled, and was taken out of Power Save Plus mode because the phone user pressed the <b>Select</b> key.</li> <li>• When the phone is repowered by the attached switch.</li> <li>• When the Phone Off Time is reached but the phone is in use.</li> </ul> <p>The range of the field is 20 to 1440 minutes.</p> <p>The default value is 60 minutes.</p>
Enable Audible Alert	<p>When enabled, instructs the phone to play an audible alert starting 10 minutes before the time that the Phone Off Time field specifies.</p> <p>The audible alert uses the phone ringtone, which briefly plays at specific times during the 10-minute alerting period. The alerting ringtone plays at the user-designated volume level. The audible alert schedule is:</p> <ul style="list-style-type: none"> <li>• At 10 minutes before power down, play the ringtone four times.</li> <li>• At 7 minutes before power down, play the ringtone four times.</li> <li>• At 4 minutes before power down, play the ringtone four times.</li> <li>• At 30 seconds before power down, play the ringtone 15 times or until the phone powers off.</li> </ul> <p>This check box applies only if the Enable Power Save Plus list box has one or more days selected.</p>
EnergyWise Domain	<p>The EnergyWise domain that the phone is in.</p> <p>The maximum length of this field is 127 characters.</p>
EnergyWise Secret	<p>The security secret password that is used to communicate with the endpoints in the EnergyWise domain.</p> <p>The maximum length of this field is 127 characters.</p>

Field	Description
Allow EnergyWise Overrides	<p>This check box determines whether you allow the EnergyWise domain controller policy to send power level updates to the phones. The following conditions apply:</p> <ul style="list-style-type: none"> <li>• One or more days must be selected in the Enable Power Save Plus field.</li> <li>• The settings in Cisco Unified Communications Manager Administration take effect on schedule even if EnergyWise sends an override.</li> </ul> <p>For example, assuming the Phone Off Time is set to 22:00 (10:00 p.m.), the value in the Phone On Time field is 06:00 (6:00 a.m.), and the Enable Power Save Plus has one or more days selected.</p> <ul style="list-style-type: none"> <li>• If EnergyWise directs the phone to turn off at 20:00 (8:00 p.m.), that directive remains in effect (assuming no phone user intervention occurs) until the configured Phone On Time at 6:00 a.m.</li> <li>• At 6:00 a.m., the phone turns on and resumes receiving the power level changes from the settings in Unified Communications Manager Administration.</li> <li>• To change the power level on the phone again, EnergyWise must reissue a new power level change command.</li> </ul> <p><b>Note</b> To disable Power Save Plus, you must uncheck the Allow EnergyWise Overrides check box. If the Allow EnergyWise Overrides remains checked but no days are selected in the Enable Power Save Plus field, Power Save Plus is not disabled.</p>

#### 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:

- *Cisco Unified Communications Manager Features and Services Guide*, “Barge and Privacy” chapter
- *Cisco Unified Communications Manager System Guide*, “Cisco Unified IP Phones” chapter

## Procedure

---

- Step 1** 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:
- Choose **System > Service Parameters**.
  - Select the appropriate Server and Service.
  - Scroll to the Clusterwide Parameters (Device - Phone) pane and set **Builtin Bridge Enable** to On.
  - Select **Save**.
- 

## Set up Do Not Disturb

When DND is turned on, either no audible rings occur during the ringing-in state of a call, or no audible or visual notifications of any type occur.

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

For more information, see “Do Not Disturb” chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

## Procedure

---

- Step 1** Using 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 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 both the Common Phone Profile window and the Phone configuration window. The Phone configuration window value takes precedence.
- BLF Status Depicts DN: Enables DND status to override busy/idle state.
- Step 4** Select **Save**.
-

## Set up monitoring and recording

The Monitoring and Recording feature allows a supervisor to monitor an active call silently. Neither party on the call can hear the supervisor. The user may receive an audible alert during a call when it is being monitored.

When a call is secure, a lock icon displays. Callers may also receive an audible alert to indicate that the call is being monitored. The connected parties may also receive an audible alert that indicates that the call is secure and is being monitored.

When an active call is being monitored or recorded, the user can receive or place intercom calls; however, if the user places an intercom call, the active call is put on hold. This action causes the recording session to terminate and the monitoring session to suspend. To resume the monitoring session, the person being monitored must resume the call.

For more information, see the “Monitoring and Recording” chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

The following procedure adds a user to the standard monitoring user groups.

### Before You Begin

The Cisco Unified Communications Manager must be configured to support Monitoring and Recording.

### Procedure

- 
- Step 1** In Cisco Unified Communications Manager Administration, select **User Management > Application User**.
  - Step 2** Check the Standard CTI Allow Call Monitoring user group and the Standard CTI Allow Call Recording user groups.
  - Step 3** Click **Add Selected**.
  - Step 4** Click **Add to User Group**.
  - Step 5** Add the user phones to the list of Application Users controlled devices.
  - Step 6** Select **Save**.
- 

## Set up Power Negotiation for LLDP

The Power Negotiation for LLDP feature allows the phone to negotiate power using Link Level Endpoint Discovery Protocol (LLDP) and Cisco Discovery Protocol (CDP).

Power Negotiation should not be disabled when the phone is connected to a switch that supports power negotiation. If disabled, the switch could shut off power to the phone.

The Power Negotiation feature is enabled by default.

### Procedure

---

- Step 1** From the Cisco Unified Communications Manager Administration, select **Device > Phone**.
  - Step 2** Locate the phone that you need to set up.
  - Step 3** In the Product Specific Configuration area, set the Power Negotiation parameter.
  - Step 4** Select **Save**.
- 

## Set up cBarge

Allows a user to join a nonprivate call on a shared phone line. cBarge adds a user to a call and converts it into a conference, allowing the user and other parties to access conference features.

For more information, see:

- *Cisco Unified Communications Manager Administration Guide*, “Cisco Unified IP Phone Configuration”
- *Cisco Unified Communications Manager System Guide*, “Cisco Unified IP Phone”
- *Cisco Unified Communications Manager Features and Services Guide*, “Barge and Privacy”

### Procedure

---

- Step 1** In Cisco Unified Communications Manager Administration, select **Device > Phone**.
  - Step 2** Locate the Single Button Barge parameter and select the required setting.  
The available settings are:
    - Off: This setting disables the Single Button Barge/cBarge feature; however, the regular Barge or cBarge features will still work.
    - CBarge: This setting enables the Single Button cBarge feature.
    - Default: Uses the Single Button Barge/cBarge setting that is in the service parameter.
  - Step 3** 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 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 > Common Phone Profile** 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**.
- 

## 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.

**Table 14: 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 Client Matter Codes

You can force users to enter a Client Matter Code (CMC) when placing a call. For more information, see the “Client Matter Codes and Forced Authorization Codes” chapter of the *Cisco Unified Communications Manager Features and Services Guide*.

### Procedure

---

- Step 1** In Cisco Unified Communications Manager Administration, select **Call Routing > Client Matter Codes**.
- Step 2** Configure the Require Client Matter Code field.  
This check box controls whether the system prompts the user for a CMC upon placing a call.
- Step 3** Select **Save**.
-



## Enable Line Status for Call Lists

To enable the Line Status for Call Lists, perform the following procedure:

### Procedure

**Step 1** Go to Cisco Unified Communications Manager Administration and choose **System > Enterprise Parameters**.

**Step 2** From the Line Status for Call Lists drop-down list box, choose the applicable profile.  
The Disabled option is selected by default.

Parameters that you set in the Product Specific Configuration area may also appear in the Device Configuration window for various devices and in the Enterprise Phone Configuration window. If you set these same parameters in these other windows as well, the setting that takes precedence is determined in the following order:

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

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

## Set up Forced Authorization Codes

You can force users to enter a Forced Authorization Code (FAC) when placing a call. For more information, see the “Client Matter Codes and Forced Authorization Codes” chapter of the *Cisco Unified Communications Manager Features and Services Guide*.

### Procedure

**Step 1** In Cisco Unified Communications Manager Administration, select **Call Routing > Forced Authorization Code**.

**Step 2** Configure the following fields.

Field	Description
Require Forced Authorization Code	Select the check box to require a user to enter an FAC.
Authorization Level	The code that the user must enter to be authorized to place the call.

**Step 3** 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**

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**

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

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

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

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

## 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 remove 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 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:
- In Cisco Unified Communications Manager Administration, choose **Device > Phone**
  - Select the appropriate IP Phones
  - Scroll to the Product Specific Configuration Layout area (Switch Port Remote Configuration or PC Port Remote Configuration) and set the parameter.
  - Select **Save**.
- Step 2** To configure the setting on multiple phones simultaneously, perform the following steps:
- In Cisco Unified Communications Manager Administration, choose **System > Enterprise Phone Configuration**
  - Configure the Remote Port Configuration parameter.
  - 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.
- 

## Set Headset Sidetone Control

When users handle calls using headsets, they may find that they are hearing feedback as they speak. This additional audio is called sidetone. If there is too much sidetone, users can hear what they are saying in the earpiece of the headset and find this sidetone distracting. The amount of sidetone varies from headset to headset.

You can adjust the sidetone level. Available sidetone levels are:

- Normal
- Low
- Very Low
- Off (Default)

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

### Procedure

- 
- Step 1** Go to Cisco Unified Communications Manager Administration and choose **Device > Phone**.
- Step 2** Find your phone from the list of phones.
- Step 3** Click on the Device Name of the phone.
- Step 4** Go to Product Specific Configuration Layout area and from the Wideband Headset UI Control drop-down list box, choose the applicable profile.  
The Off option is selected by default (should be enabled only if the user headset supports wideband).  
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 5** Select **Save**.
- 

## Enable Actionable Incoming Call Alert

When this feature is enabled, an actionable alert displays when there is an incoming call. The alert replaces the traditional incoming call pop-up notification, and the user must respond to the alert.



**Note** If both the Custom Line Filters and Actionable Incoming Call Alert features are enabled, actionable call alerts apply only to the lines that are covered by filters.

---

### Procedure

- 
- Step 1** Go to Cisco Unified Communications Manager Administration and choose one of the following:
- **System > Enterprise Phone Configuration**
  - **Device > Device Settings > Common Phone Profile**
  - **Device > Phone**
- Step 2** Locate the Actionable Incoming Call Alert field and set the field to the appropriate setting.  
The possible field values are:

- Disabled: (default) The actionable incoming call alert is disabled. The traditional incoming call pop-up alert displays.
- Show for all Incoming Call: The actionable incoming call alert displays for all calls regardless of visibility.
- Show for Invisible Incoming Call: The actionable incoming call alert displays for calls not shown on the phone. This parameter behaves similarly to the incoming call alert pop-up notification.

If you also configure this field in the other windows, the setting precedence is:

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

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

---

## Enable Call History for Shared Line

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

### Procedure

---

- Step 1** Go to Cisco Unified CM Administration and choose **Device > Phone**.
- Step 2** Find your phone from the list of phones associated with the Cisco Unified CM.
- Step 3** Click on the Device Name of the phone.
- Step 4** Go to Product Specific Configuration Layout area and from the Logging Display drop-down list box, choose the applicable profile.  
The Disabled option is selected by default.

Parameters that you set in the Product Specific Configuration area may also appear in the Device Configuration window for various devices and in the Enterprise Phone Configuration window.

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

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

## 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 **Apply Config**.

## UCR 2008 setup

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

**Table 15: UCR 2008 parameter location**

Parameter	Administration path
FIPS Mode	<b>Device &gt; Device Settings &gt; Common Phone Profile</b>
	<b>System &gt; Enterprise Phone Configuration</b>
SSH Access	<b>Device &gt; Phone</b>
	<b>Device &gt; Device Settings &gt; Common Phone Profile</b>
Web Access	<b>Device &gt; Phone</b>
80-bit SRTP	<b>Device &gt; Device Settings &gt; Common Phone Profile</b>
	<b>System &gt; Enterprise Phone Configuration</b>
IP Addressing Mode	<b>Device &gt; Device Settings &gt; Common Device Configuration</b>
IP Addressing Mode Preference for Signaling	<b>Device &gt; Device Settings &gt; Common Device Configuration</b>

## Set up UCR 2008 in Common Device Configuration

Use this procedure to set the following UCR 2008 parameters:

- IP Addressing Mode
- IP Addressing Mode Preference for Signaling

### Procedure

---

- Step 1** In Cisco Unified Communications Manager Administration, choose **Device > Device Settings > Common Device Configuration**.
- Step 2** Set the IP Addressing Mode parameter.
- Step 3** Set the IP Addressing Mode Preference for Signaling parameter.
- Step 4** Select **Save**.
- 

## Set up UCR 2008 in Common Phone Profile

Use this procedure to set the following UCR 2008 parameters:

- FIPS Mode
- SSH Access
- 80-bit SRTCP

### Procedure

---

- Step 1** In Cisco Unified Communications Manager Administration, choose **Device > Device Settings > Common Phone Profile**.
- Step 2** Set the FIPS Mode parameter to **Enabled**.
- Step 3** Set the SSH Access parameter to **Disabled**.
- Step 4** Set the 80-bit SRTCP parameter to **Enabled**.
- Step 5** Select **Save**.
- 

## Set up UCR 2008 in Enterprise Phone Configuration

Use this procedure to set the following UCR 2008 parameters:

- FIPS Mode
- 80-bit SRTCP



### Procedure

---

- Step 1** In Cisco Unified Communications Manager Administration, choose **System > Enterprise Phone Configuration**.
  - Step 2** Set the FIPS Mode parameter to **Enabled**.
  - Step 3** Set the 80-bit SRTCP parameter to **Enabled**.
  - Step 4** Select **Save**.
- 

## Set up UCR 2008 in Phone

Use this procedure to set the following UCR 2008 parameters:

- SSH Access
- Web Access

### Procedure

---

- Step 1** In Cisco Unified Communications Manager Administration, choose **Device > Phone**.
  - Step 2** Set the SSH Access parameter to **Disabled**.
  - Step 3** Set the Web Access parameter to **Disabled**.
  - Step 4** Select **Save**.
- 

## Set up softkey template

You can associate up to 18 softkeys with applications that are supported by the Cisco IP Phone 7821, 7841, and 7961. An application that supports softkeys can have one or more standard softkey templates associated with it.

Cisco Unified Communications Manager supports the Standard User and Standard Feature softkey template. 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.

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

The phones do not support all the softkeys that are configurable in Softkey Template Configuration on Cisco Unified Communications Manager Administration. The following table lists the features, softkeys that can be configured on a softkey template, and note whether it is supported on the Cisco IP Phone 7821, 7841, and 7961.

**Table 16: Configurable softkeys**

<b>Feature</b>	<b>Configurable softkeys in the Softkey Template configuration</b>	<b>Support status</b>	<b>Notes</b>
Answer	Answer (Answer)	Yes	-
Barge	Barge (Barge)	No	Configure as a programmable line key or as a softkey.
Call Back	Call Back (CallBack)	Yes	-
Call Forward All	Forward All (cfwdAll)	Yes	Phone displays Fwd ALL or Fwd Off.
Call Park	Call Park (Park)	Yes	-
Call Pickup	Pick Up (Pickup)	Yes	Configure as a programmable line key or as a softkey.
cBarge	Conference Barge (cBarge)	Yes	Configure as a programmable line key or as a softkey.
Conference	Conference (Confm)	No	Conference is a dedicated button.
Conference List	Conference List (ConfList)	No	Phone displays Detail.
Divert	ImmediateDivert (iDivert)	Yes	Phone displays Divert.
Do Not Disturb	Toggle Do Not Disturb (DND)	Yes	Configure as a programmable line button or softkey.
End Call	End Call (EndCall)	Yes	Phone displays Cancel if the call is not answered.
Group Pickup	Group PickUp (GPickUp)	Yes	Configure as a programmable line button or softkey
Hold	Hold (Hold)	Yes	Hold is a dedicated button.
Hunt Group	HLog (HLog)	Yes	Configure as a programmable feature button.
Join	Join (Join)	Yes	-
Malicious Call Identification	Toggle Malicious Call Identification (MCID)	Yes	Configure as a programmable feature button or softkey.

Feature	Configurable softkeys in the Softkey Template configuration	Support status	Notes
Meet Me	Meet Me (MeetMe)	Yes	Configure as a programmable feature button or softkey.
Mobile Connect	Mobility (Mobility)	Yes	Configure as a programmable feature button or softkey.
New Call	New Call (NewCall)	Yes	Phone displays <code>New Call</code> .
Other Pickup	Other Pickup (oPickup)	Yes	Configure as a programmable feature button or softkey.
PLK Support for Queue Statistics	Queue Status	Yes	-
Quality Reporting Tool	Quality Reporting Tool (QRT)	Yes	Configure as a programmable feature button or softkey.
Redial	Redial (Redial)	Yes	-
Remove Last Conference Participant	Remove Last Conference Participant (Remove)	Yes	Phone displays <code>Remove</code> when a participant is selected.
Resume	Resume (Resume)	Yes	-
Speed Dial	Abbreviated Dial (AbbrDial)	Yes	Phone displays <code>SpeedDial</code> .
Transfer	Direct Transfer (DirTrfr)	No	Transfer is a dedicated button. Configure Transfer (Direct Transfer policy) in the Product Specific Configuration Layout section in Phone Configuration.
Video Mode Command	Video Mode Command (VidMode)	No	-

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

### Procedure

---

- Step 1** In Cisco Unified Communications Manager, select **Device > Device Settings > Softkey Template**.
  - Step 2** Locate the template that you want to change.
  - Step 3** Select Configure Softkey Layout from the Related Links list and click **Go**.
  - Step 4** Configure the softkey positions.
  - Step 5** Select **Save** to save the layout.
  - Step 6** Select **Save** to save the template.
  - Step 7** Select **Apply Config** to apply the template to the phones.
- 

## Set 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 and click the link.
  - Step 3** Navigate to Minimum Ring Volume and choose a value between 0 and 14.
  - Step 4** Click **Save**.
- 

## Set up Join and Direct Transfer Policy

Some JTAPI/TAPI applications are not compatible with the Join and Direct Transfer feature implementation on the Cisco IP Phone. In order for these applications to control and monitor these phones, you must configure the Join and Direct Transfer Policy to disable join and direct transfer on the same line or possibly across lines.

Because this parameter can be configured in three different windows, 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

When you change the setting of the Join and Direct Transfer Policy parameter, you must check the Override Common Settings box for the setting to take effect. The default policy is to have Same line, across line enabled for join and direct transfer.

To determine the proper setting for this parameter, refer to the documentation of the JTAPI/TAPI application.

### Procedure

- 
- Step 1** To configure the policy for all phones on the system, choose **System > Enterprise Phone Configurations**.
  - Step 2** To configure the policy to a group of phones, choose **Device > Device Settings > Common Phone Profile**.
  - Step 3** To configure the policy on an individual phone, configure the Join and Direct Transfer Policy in the Phone Configuration for the specific phone in **Device > Phone**.
  - Step 4** Set the Join and Direct Transfer Policy field.
  - Step 5** Check the Override Common Settings box.
  - Step 6** Select **Save**.
- 

## Set up HTTPS for Phone Services

You can increase security by requiring that communications use HTTPS instead of HTTP.




---

**Note** IP Phones can be HTTPS clients; they cannot be HTTPS servers.

---

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

### Procedure

- 
- Step 1** In Cisco Unified Communications Manager Administration, select **Device > Phone** or **System > Enterprise Phone Configuration**.
  - Step 2** Enable the HTTPS Service parameter
  - Step 3** Select **Save**.
- 

## Phone button templates

Phone button templates let you assign speed dials and call-handling features to programmable buttons. Call-handling features that can be assigned to buttons include Answer, Mobility, and All Calls.

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

### Modify phone button template

For more information about IP Phone services, see “Cisco Unified IP Phone Services Configuration” chapter in the *Cisco Unified Communications Manager Administration Guide*. For more information about configuring line buttons, see “Cisco Unified IP Phone Configuration” chapter and “Configuring Speed-Dial Buttons” section in the *Cisco Unified Communications Manager Administration Guide*.

### Procedure

---

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

## Assign phone button template for All Calls

Assign an All Calls button in the phone template for users with multiple shared lines.

When you configure an All Calls button on the phone, users use the All Calls button to:

- See a consolidated list of current calls from all lines on the phone.
- See (under Call History) a list of all missed calls from all lines on the phone.
- Place a call on the user's primary line when the user goes off-hook. All Calls automatically defaults to the user primary line for any outgoing call.

### Procedure

---

- Step 1** Modify the phone button template to include the All Calls button.
- Step 2** Assign the template to the phone.
- 

## Set up PAB or Speed Dial as IP phone service

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.

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

## Procedure

- 
- Step 1** From Cisco Unified Communications Manager Administration, choose **Device > Device Settings > Phone Services**.  
The Find and List IP Phone Services window displays.
- Step 2** Click **Add New**.  
The IP Phone Services Configuration window displays.
- Step 3** Enter the following settings:
- Service Name and ASCII Service Name: Enter **Personal Address Book**.
  - Service Description: Enter an optional description of the service.
  - Service URL  
For PAB, enter the following URL:  
**http://<Unified CM-server-name>:8080/ccmpd/login.do?name=#DEVICENAME#&service=pab**  
For Fast Dial, enter the following URL:  
**http://<Unified-CM-server-name>:8080/ccmpd/login.do?name=#DEVICENAME#&service=fd**
  - Secure Service URL  
For PAB, enter the following URL:  
**https://<Unified CM-server-name>:8443/ccmpd/login.do?name=#DEVICENAME#&service=pab**  
For Fast Dial, enter the following URL:  
**https://<Unified-CM-server-name>:8443/ccmpd/login.do?name=#DEVICENAME#&service=fd**
  - Service Category: Select **XML Service**.
  - Service Type: Select **Directories**.
  - Enable: Select the check box.  
*http://<IP\_address> or https://<IP\_address> (Depends on the protocol that the Cisco IP Phone supports.)*
- Step 4** Select **Save**.  
You can add, update, or delete service parameters as described in the “Cisco Unified IP Phone Services Configuration” chapter in the *Cisco Unified Communications Manager Administration Guide*.
- Note** If you change the service URL, remove an IP Phone service parameter, or change the name of a phone service parameter for a phone service to which users are subscribed, you must click **Update Subscriptions** to update all currently subscribed users with the changes; otherwise, users must resubscribe to the service to rebuild the correct URL.
- 

## Modify phone button template for PAB or Fast Dial

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, see “Cisco Unified IP Phone Services Configuration” chapter in the *Cisco Unified Communications Manager Administration Guide*. For more information about configuring line buttons, see “Cisco Unified IP Phone Configuration” chapter and “Configuring Speed-Dial Buttons” section in the *Cisco Unified Communications Manager Administration Guide*.

### Procedure

---

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





## Corporate and Personal Directory setup

---

- [Corporate Directory setup, page 137](#)
- [Personal Directory setup, page 137](#)
- [User personal directory entries setup, page 138](#)

### 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 “Understanding Directory Numbers” in the *Cisco Unified Communications Manager System Guide*.

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

### Personal Directory setup

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 TABSynch tool to synchronize their PABs with Microsoft Windows Address Book (WAB). Customers who want to use the Microsoft Outlook Address Book (OAB) should begin by importing the data from the OAB into the WAB. TabSync can then be used to synchronize the WAB with Personal Directory. For instructions about TABSync, see [Download Cisco IP Phone Address Book Synchronizer, on page 138](#) and [Set up synchronizer, on page 139](#).

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 [Self Care Portal management, on page 53](#) 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 138](#).

## 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 138](#) 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.  
The publisher dialog box displays.
  - Step 3** Select **Run**.  
The Welcome to the InstallShield Wizard for Cisco Unified CallManager Personal Address Book Synchronizer window displays.
  - Step 4** Select **Next**.  
The License Agreement window displays.
  - Step 5** Read the license agreement information, and select the **I Accept**. Select **Next**.  
The Destination Location window displays.
  - Step 6** Choose the directory in which you want to install the application and select **Next**.  
The Ready to Install window displays.
  - Step 7** Select **Install**.  
The installation wizard installs the application to your computer. When the installation is complete, the InstallShield Wizard Complete window displays.
  - Step 8** Select **Finish**.
  - Step 9** To complete the process, follow the steps in [Set up synchronizer, on page 139](#).
- 

**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**.  
The Cisco Unified CallManager User Information window displays.

- 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**. The Configure Cisco Unified CallManager Server Information window displays.
- Step 5** Enter the IP address or host name and the port number of the Cisco Unified Communications Manager server and select **OK**.  
If you do not have this information, contact your system administrator.
- Step 6** To start the directory synchronization process, select **Synchronize**.  
The Synchronization Status window provides the status of the address book synchronization. If you chose the user intervention for duplicate entries rule and you have duplicate address book entries, the Duplicate Selection window displays.
- Step 7** Choose the entry that you want to include in your Personal Address Book and select **OK**.
- Step 8** When synchronization is complete, select **Exit** to close the Cisco Unified CallManager Address Book Synchronizer.
- Step 9** To verify whether the synchronization worked, sign in to your Self Care Portal and choose **Personal Address Book**. The users from your Windows address book should be listed.
-



# PART **V**

## **Cisco IP Phone Troubleshooting**

- [Monitoring phone systems, page 143](#)
- [Troubleshooting , page 169](#)
- [Maintenance, page 189](#)
- [International User Support, page 195](#)





## Monitoring phone systems

---

- [Monitoring phone systems overview, page 143](#)
- [Cisco IP Phone status , page 143](#)
- [Cisco IP Phone web page, page 155](#)

### Monitoring phone systems overview

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

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

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

You can also obtain much of this information directly from a phone. For more information, see [xref](#) .

For more information about troubleshooting the Cisco Unified IP Phone, see [xref](#) .

This chapter includes these topics:

### Cisco IP Phone status

The following sections describes how to view model information, status messages, and network statistics on the Cisco IP Phone 7821, 7841, and 7861.

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

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

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

For more information about troubleshooting the Cisco Unified IP Phone 7821, 7841, and 7861, see [Troubleshooting](#) , on page 169.

## Display Model 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**.
- 

## Display Status menu

To display the Status menu, perform these steps:

### Procedure

---


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

## Display Status Messages window

To display the Status Messages screen, follow these steps:



## Procedure

- 
- Step 1** Press **Applications** .
- Step 2** Select **Admin Settings**.
- Step 3** Select **Status**.
- Step 4** Select **Status Messages**.
- Step 5** To remove current status messages, press **Clear List**.
- Step 6** To exit the Status Messages screen, press **Exit**.
- 

### Status messages fields

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

**Table 17: Status messages on the Cisco IP Phone**

Message	Description	Possible explanation and action
CFG TFTP Size Error	The configuration file is too large for file system on the phone.	Power cycle the phone.
Checksum Error	Downloaded software file is corrupted.	Obtain a new copy of the phone firmware and place it in the TFTPPath directory. You should only copy files into this directory when the TFTP server software is shut down; otherwise, the files may be corrupted.
CTL and ITL installed	The CTL and ITL files are installed on the phone.	None. This message is informational only. Neither the CTL file nor the ITL file was installed previously.  For more information about the trust list, see <i>Cisco Unified Communications Manager Security Guide</i> .
CTL Installed	A certificate trust list (CTL) file is installed in the phone.	None. This message is informational only. The CTL file was not installed previously.  For more information about the CTL file, see the <i>Cisco Unified Communications Manager Security Guide</i> .
CTL update failed	The phone could not update the certificate trust list (CTL) file.	Problem with the CTL file on the TFTP server.  For more information, see the <i>Cisco Unified Communications Manager Security Guide</i> .

Message	Description	Possible explanation and action
DHCP timeout	DHCP server did not respond.	<p>Network is busy - The errors should resolve themselves when the network load reduces.</p> <p>No network connectivity between the DHCP server and the phone: Verify the network connections.</p> <p>DHCP server is down: Check configuration of DHCP server.</p> <p>Errors persist: Consider assigning a static IP address.</p>
DNS timeout	DNS server did not respond.	<p>Network is busy: The errors should resolve themselves when the network load reduces.</p> <p>No network connectivity between the DNS server and the phone: Verify the network connections.</p> <p>DNS server is down: Check configuration of the DNS server.</p>
DNS unknown host	DNS could not resolve the name of the TFTP server or Cisco Unified Communications Manager.	<p>Verify that the host names of the TFTP server or Cisco Unified Communications Manager are configured properly in DNS.</p> <p>Consider using IP addresses rather than host names</p>
Duplicate IP	Another device is using the IP address that is assigned to the phone.	<p>If the phone has a static IP address, verify that you did not assigned a duplicate IP address.</p> <p>If you are using DHCP, check the DHCP server configuration.</p>
Erasing CTL and ITL files	Erasing CTL or ITL file.	<p>None. This message is informational only.</p> <p>For more information about the CTL and ITL files, see the <i>Cisco Unified Communications Manager Security Guide</i>.</p>

Message	Description	Possible explanation and action
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 <Cfg File>	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 does not exist in 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.</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.</li> </ul>
File Not Found <CTLFile.tlv>	This message displays on the phone when the Cisco Unified Communications Manager cluster is not in secure mode.	No impact; the phone can still register to Cisco Unified Communications Manager.
IP address released	The phone is configured to release the IP address.	The phone remains idle until it is power cycled or until you reset the DHCP address.

Message	Description	Possible explanation and action
ITL installed	The ITL file is installed in the phone.	None. This message is informational only. The ITL file was not installed previously.  For more information about the ITL file, see <i>Cisco Unified Communications Manager Security Guide</i> .
Load rejected HC	The application that was downloaded is not compatible with the phone hardware.	Occurs if you attempted to install a version of software on this phone that did not support hardware changes on this phone.  Check the load ID that is assigned to the phone (from Cisco Unified Communications Manager, choose <b>Device &gt; Phone</b> ). Reenter the load that displays on the phone.
No default router	DHCP or static configuration did not specify a default router.	If the phone has a static IP address, verify that the default router is configured.  If you are using DHCP, the DHCP server has not provided a default router. Check the DHCP server configuration.
No DNS server IP	A name was specified but DHCP or static IP configuration did not specify a DNS server address.	If the phone has a static IP address, verify that the DNS server is configured.  If you are using DHCP, the DHCP server has not provided a DNS server. Check the DHCP server configuration.
No Trust List installed	The CTL file or the ITL file is not installed on the phone.	The trust list is not configured on the Cisco Unified Communications Manager, which does not support security by default.  For more information about the trust list, see the <i>Cisco Unified Communications Manager Security Guide</i> .
Restart requested by Cisco Unified Communications Manager	The phone is restarting due to on a request from Cisco Unified Communications Manager.	Configuration changes were likely made to the phone in Cisco Unified Communications Manager, and <b>Apply</b> was pressed so that the changes take effect.
TFTP access error	TFTP server is pointing to a directory that does not exist.	If you are using DHCP, verify that the DHCP server is pointing to the correct TFTP server.  If you are using static IP addresses, check configuration of TFTP server.
TFTP error	The phone does not recognize an error code that the TFTP server provided.	Contact Cisco TAC.


Message	Description	Possible explanation and action
TFTP timeout	TFTP server did not respond.	<p>Network is busy: The errors should resolve themselves when the network load reduces.</p> <p>No network connectivity between the TFTP server and the phone: Verify the network connections.</p> <p>TFTP server is down: Check configuration of TFTP server.</p>
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.
Trust List update failed	Update of the CTL and ITL files failed.	<p>Phone has CTL and ITL files installed and it failed to update the new CTL and ITL files.</p> <p>Possible reasons for failure:</p> <ul style="list-style-type: none"> <li>• Network failure occurred.</li> <li>• TFTP server was down.</li> <li>• The new security token that was used to sign CTL file and the TFTP certificate that was used to sign ITL file are introduced, but are not available in the current CTL and ITL files in the phone.</li> <li>• Internal phone failure occurred.</li> </ul> <p>Possible solutions:</p> <ul style="list-style-type: none"> <li>• Check network connectivity.</li> <li>• Check whether the TFTP server is active and functioning normally.</li> <li>• If the Transactional Vsam Services (TVS) server is supported on Cisco Unified Communications Manager, check whether the TVS server is active and functioning normally.</li> <li>• Verify whether the security token and the TFTP server are valid.</li> </ul> <p>Manually delete the CTL and ITL files if all the preceding solutions fail; reset the phone.</p>
Trust List updated	The CTL file, the ITL file, or both files are updated.	<p>None. This message is informational only.</p> <p>For more information about the trust list, see the <i>Cisco Unified Communications Manager Security Guide</i>.</p>

Message	Description	Possible explanation and action
Version error	The name of the phone load file is incorrect.	Make sure that the phone load file has the correct name.
XmlDefault.cnf.xml, or .cnf.xml corresponding to the phone device name	Name of the configuration file.	None. This message indicates the name of the configuration file for the phone.

### Display Network Statistics window

To display the Network Statistics screen, perform these steps:

#### Procedure

- 
- Step 1** Press **Applications**.
  - Step 2** Select **Admin Settings**.
  - Step 3** Select **Status**.
  - Step 4** Select **Status > Network Statistics**.
  - Step 5** To reset the Rx Frames, Tx Frames, and Rx Broadcasts statistics to 0, press **Clear**.
  - Step 6** To exit the Network Statistics screen, press **Back** .
- 

#### Network Statistics fields

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

**Table 18: Network Statistics Fields**

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 auto-negotiated a full-duplex, 100-Mbps connection)
Port 2	Link state and connection of the Network port
IPv4	Information on the DHCP status. This includes the following states: <ul style="list-style-type: none"> <li>• CDP BOUND</li> <li>• CDP INIT</li> <li>• DHCP BOUND</li> <li>• DHCP DISABLED</li> <li>• DHCP INIT</li> <li>• DHCP INVALID</li> <li>• DHCP REBINDING</li> <li>• DHCP REBOOT</li> <li>• DHCP RENEWING</li> <li>• DHCP REQUESTING</li> <li>• DHCP RESYNC</li> <li>• DHCP UNRECOGNIZED</li> <li>• DHCP WAITING COLDBOOT TIMEOUT</li> <li>• SET DHCP COLDBOOT</li> <li>• SET DHCP DISABLED</li> <li>• DISABLED DUPLICATE IP</li> <li>• SET DHCP FAST</li> </ul>

## 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.

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

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

### Procedure

- 
- Step 1** Press **Applications**.
  - Step 2** Select **Admin Settings**.
  - Step 3** Select **Status**.
  - Step 4** Select **Call Statistics**.
  - Step 5** To exit the Call Statistics screen, press **Exit**.
- 

### Call Statistics fields

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

**Table 19: Call Statistics items for the Cisco IP Phone**

Item	Description
Rcvr Codec	Type of received voice stream (RTP streaming audio from codec): G.729, G.722, G.711 mu-law, G.711 A-law, and iLBC.
Sender Codec	Type of transmitted voice stream (RTP streaming audio from codec): G.729, G.722, G.711 mu-law, G.711 A-law, and iLBC.
Rcvr Size	Size of voice packets, in milliseconds, in the receiving voice stream (RTP streaming audio).
Sender Size	Size of voice packets, in milliseconds, in the transmitting voice stream.
Rcvr Packets	Number of RTP voice packets that were received since voice stream opened. <b>Note</b> This number is not necessarily identical to the number of RTP voice packets that were received since the call began because the call might have been placed on hold.



Item	Description
Sender Packets	Number of RTP voice packets that were transmitted since voice stream opened.  <b>Note</b> This number is not necessarily identical to the number of RTP voice packets that were transmitted since the call began because the call might have been placed on hold.
Avg Jitter	Estimated average RTP packet jitter (dynamic delay that a packet encounters when going through the network), in milliseconds, that was observed since the receiving voice stream opened.
Max Jitter	Maximum jitter, in milliseconds, that was observed since the receiving voice stream opened.
Revr Discarded	Number of RTP packets in the receiving voice stream that were discarded (bad packets, too late, and so on).  <b>Note</b> The phone discards payload type 19 comfort noise packets that Cisco Gateways generate, because they increment this counter.
Revr Lost Packets	Missing RTP packets (lost in transit).
<b>Voice-Quality Metrics</b>	
MOS LQK	Score that is an objective estimate of the mean opinion score (MOS) for listening quality (LQK) that rates from 5 (excellent) to 1 (bad). This score is based on audible concealment events due to frame loss in the preceding eight-second interval of the voice stream.  <b>Note</b> The MOS LQK score can vary based on the type of codec that the Cisco IP Phone uses.
Avg MOS LQK	Average MOS LQK score that was observed for the entire voice stream.
Min MOS LQK	Lowest MOS LQK score that was observed from the start of the voice stream.
Max MOS LQK	Baseline or highest MOS LQK score that was observed from start of the voice stream.  These codecs provide the following maximum MOS LQK score under normal conditions with no frame loss: <ul style="list-style-type: none"> <li>• G.711 yields a score of 4.5.</li> <li>• G.729 A /AB yields a score of 3.7.</li> </ul>
MOS LQK Version	Version of the Cisco proprietary algorithm that is used to calculate MOS LQK scores.
Cumulative Conceal Ratio	Total number of concealment frames divided by total number of speech frames that were received from start of the voice stream.

Item	Description
Interval Conceal Ratio	Ratio of concealment frames to speech frames in preceding 3-second interval of active speech. If using voice activity detection (VAD), a longer interval might be required to accumulate 3 seconds of active speech.
Max Conceal Ratio	Highest interval concealment ratio from start of the voice stream.
Conceal Secs	Number of seconds that have concealment events (lost frames) from the start of the voice stream (includes severely concealed seconds).
Severely Conceal Secs	Number of seconds that have more than 5 percent concealment events (lost frames) from the start of the voice stream.
Latency	Estimate of the network latency, expressed in milliseconds. Represents a running average of the round-trip delay, measured when RTCP receiver report blocks are received.

### Display Security Configuration window

You can view information about the security on the phone. To display the Security Configuration screen, follow these steps.

#### Procedure

- 
- Step 1** Press **Applications**.
  - Step 2** Select **Admin Settings**.
  - Step 3** Select **Security**.
  - Step 4** To exit, press **Exit**.
- 

### Security Configuration fields

The Security Configuration screen displays these items.

**Table 20: Security Configuration items**

Item	Description
Security Mode	Displays the security mode that is set for the phone.
LSC	Indicates whether a locally significant certificate (used for the security features) is installed on the phone or is not installed on the phone.
Trust List	The Trust List is a top-level menu that provides submenus for the CTL Signature and Call manager/TFTP Server.
802.1x Authentication	Allows you to enable 802.1X authentication for the phone.

## 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. For more information, see [Display Model Information window, on page 144](#).

### Related Topics

[Control phone web page access, on page 126](#)

## Access Web Page for phone


To access the web page for a Cisco IP Phone, follow these steps:



### Note

If you cannot access the web page, it may be disabled by default. For more information, see xref .

### Procedure

- 
- Step 1** Obtain the IP address of the Cisco IP Phone by using one of these methods:
- a) Search for the phone in Cisco Unified Communications Manager Administration by choosing **Device > Phone**. Phones that register with Cisco Unified Communications Manager display the IP address on the Find and List Phones window and at the top of the Phone Configuration window.
  - b) On the Cisco IP Phone, press **Applications** , choose **Admin Settings > Network Setup > Ethernet Setup > IPv4 Setup**, and then scroll to the IP Address option.
- Step 2** Open a web browser and enter the following URL, where *IP\_address* is the IP address of the Cisco IP Phone: **http://<IP\_address>** or **https://<IP\_address>** (depending on the protocol supported by the Cisco IP Phone)
-

## Device information

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



**Note**

Some of the items in the following table do not apply to all phone models.

To display the Device Information area, access the web page for the phone as described in [Access Web Page for phone](#), on page 155, and then click the **Device Information** hyperlink.

**Table 21: Device Information Area Items**

Item	Description
MAC Address	Media Access Control (MAC) address of the phone.
Host Name	Unique, fixed name that is automatically assigned to the phone based on the MAC address.
Phone DN	Directory number that is assigned to the phone.
Version	Identifier of the firmware that is running on the phone.
Hardware Revision	Revision value of the phone hardware.
Serial Number	Unique serial number of the phone.
Model Number	Model number of the phone.
Message Waiting	Indicates whether a voice message is waiting on the primary line for this phone.
UDI	Displays the following Cisco Unique Device Identifier (UDI) information about the phone: <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>• Serial Number: Displays the unique serial number of the phone.</li> </ul>
Time	Time for the Date/Time Group to which the phone belongs. This information comes from Cisco Unified Communications Manager.
Time Zone	Time zone for the Date/Time Group to which the phone belongs. This information comes from Cisco Unified Communications Manager.

Item	Description
Date	Date for the Date/Time Group to which the phone belongs. This information comes from Cisco Unified Communications Manager.

## Network setup

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

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

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

**Table 22: Network Setup Area Items**

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

Item	Description
CUCM Server 1–5	<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 shows 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 IP Phone services.
DHCP Enabled	Indicates whether the phone uses DHCP.
DHCP Address Released	Indicates the setting of the DHCP Address Released option on the phone Network Configuration menu.
Alternate TFTP	Indicates whether the phone is using an alternative TFTP server.
Idle URL	URL that the phone displays when the phone is idle for the time that the Idle URL Time field specifies and no menu is open.
Idle URL Time	Number of seconds that the phone is idle and no menu is open before the XML service that the Idle URL specifies activates.
Proxy Server URL	URL of proxy server, which makes HTTP requests to nonlocal host addresses on behalf of the phone HTTP client and provides responses from the nonlocal host to the phone HTTP client.

Item	Description
Authentication URL	URL that the phone uses to validate requests that are made to the phone web server.
SW Port Setup	Speed and duplex of the switch port, where: <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>
PC 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 PC port</li> </ul>
TFTP Server 2	Backup TFTP server that the phone uses if the primary TFTP server is unavailable.
User Locale	User locale that associates with the phone user. Identifies a set of detailed information to support users, including language, font, date and time formatting, and alphanumeric keyboard text information.
Network Locale	Network locale that associates with the phone user. Identifies a set of detailed information to support the phone in a specific location, including definitions of the tones and cadences that the phone uses.
Headset Enabled	Indicates whether the Headset button is enabled on the phone.
User Locale Version	Version of the user locale that is loaded on the phone.
Network Locale Version	Version of the network locale that is loaded on the phone.
PC Port Disabled	Indicates whether the PC port on the phone is enabled or disabled.
Speaker Enabled	Indicates whether the speakerphone is enabled on the phone.

Item	Description
GARP Enabled	Indicates whether the phone learns MAC addresses from Gratuitous ARP responses.
Voice VLAN Enabled	Indicates whether the phone allows a device that is attached to the PC port to access the Voice VLAN.
DSCP for Call Control	DSCP IP classification for call control signaling.
DSCP for Configuration	DSCP IP classification for any phone configuration transfer.
DSCP for Services	DSCP IP classification for phone-based services.
Security Mode	Security mode that is set for the phone.
Web Access Enabled	Indicates whether web access is enabled (Yes) or disabled (No) for the phone.
Span to PC Port	Indicates whether the phone forwards packets that are transmitted and received on the network port to the access port.
PC VLAN	VLAN that identifies and removes 802.1P/Q tags from packets that are sent to the PC.
CDP on PC Port	Indicates whether CDP is supported on the PC port (default is enabled). When CDP is disabled in Cisco Unified Communications Manager, a warning is displayed to indicate that disabling CDP on the PC port prevents CVTA from working. The current PC and switch port CDP values are shown in the Settings menu.
CDP on SW Port	Indicates whether CDP support exists on the switch port (default is enabled). Enable CDP on the switch port for VLAN assignment for the phone, power negotiation, QoS management, and 802.1x security. Enable CDP on the switch port when the phone connects to a Cisco switch. When CDP is disabled in Cisco Unified Communications Manager, a warning is presented, indicating that CDP should be disabled on the switch port only if the phone connects to a non-Cisco switch. The current PC and switch port CDP values are shown on the Settings menu.
LLDP-MED: SW Port	Indicates whether Link Layer Discovery Protocol Media Endpoint Discovery (LLDP-MED) is enabled on the switch port.
LLDP: PC Port	Indicates whether Link Layer Discovery Protocol (LLDP) is enabled on the PC port.



Item	Description
LLDP Power Priority	Advertises the phone power priority to the switch, thus enabling the switch to appropriately provide power to the phones. Settings include: <ul style="list-style-type: none"> <li>• Unknown: This is the default value.</li> <li>• Low</li> <li>• High</li> <li>• Critical</li> </ul>
LLDP Asset ID	Identifies the asset ID that is assigned to the phone for inventory management.

### Network statistics

The following Network Statistics hyperlinks on a phone web page provide information about network traffic on the phone:

- Ethernet Information: Displays information about Ethernet traffic.
- Access area: Displays information about network traffic to and from the PC port on the phone.
- Network area: Displays information about network traffic to and from the network port on the phone.

To display a network statistics area, access the web page for the phone, and then click the **Ethernet Information**, the **Access**, or the **Network** hyperlink.

### Related Topics

[Access Web Page for phone, on page 155](#)

### *Ethernet Information web page*

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

**Table 23: Ethernet Information items**

Item	Description
Tx Frames	Total number of packets that the phone transmits.
Tx broadcast	Total number of broadcast packets that the phone transmits.
Tx multicast	Total number of multicast packets that the phone transmits.
Tx unicast	Total number of unicast packets that the phone transmits.
Rx Frames	Total number of packets received by the phone.
Rx broadcast	Total number of broadcast packets that the phone receives..
Rx multicast	Total number of multicast packets that the phone receives.

Item	Description
Rx unicast	Total number of unicast packets that the phone receives.
Rx PacketNoDes	Total number of shed packets that the no Direct Memory Access (DMA) descriptor causes.

### Access Area and Network Area web pages

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

**Table 24: Access Area and Network Area items**

Item	Description
Rx totalPkt	Total number of packets that the phone received.
Rx crcErr	Total number of packets that were received with CRC failed.
Rx alignErr	Total number of packets between 64 and 1522 bytes in length that were received and that have a bad Frame Check Sequence (FCS).
Rx multicast	Total number of multicast packets that the phone received.
Rx broadcast	Total number of broadcast packets that the phone received.
Rx unicast	Total number of unicast packets that the phone received.
Rx shortErr	Total number of received FCS error packets or Align error packets that are less than 64 bytes in size.
Rx shortGood	Total number of received good packets that are less than 64 bytes size.
Rx longGood	Total number of received good packets that are greater than 1522 bytes in size.
Rx longErr	Total number of received FCS error packets or Align error packets that are greater than 1522 bytes in size.
Rx size64	Total number of received packets, including bad packets, that are between 0 and 64 bytes in size.
Rx size65to127	Total number of received packets, including bad packets, that are between 65 and 127 bytes in size.
Rx size128to255	Total number of received packets, including bad packets, that are between 128 and 255 bytes in size.
Rx size256to511	Total number of received packets, including bad packets, that are between 256 and 511 bytes in size.

<b>Item</b>	<b>Description</b>
Rx size512to1023	Total number of received packets, including bad packets, that are between 512 and 1023 bytes in size.
Rx size1024to1518	Total number of received packets, including bad packets, that are between 1024 and 1518 bytes in size.
Rx tokenDrop	Total number of packets that were dropped due to lack of resources (for example, FIFO overflow).
Tx excessDefer	Total number of packets that were delayed from transmitting due to busy medium.
Tx lateCollision	Number of times that collisions occurred later than 512 bit times after the start of packet transmission.
Tx totalGoodPkt	Total number of good packets (multicast, broadcast, and unicast) that the phone received.
Tx Collisions	Total number of collisions that occurred while a packet was transmitted.
Tx excessLength	Total number of packets that were not transmitted because the packet experienced 16 transmission attempts.
Tx broadcast	Total number of broadcast packets that the phone transmitted.
Tx multicast	Total number of multicast packets that the phone transmitted.
LLDP FramesOutTotal	Total number of LLDP frames that the phone sent out.
LLDP AgeoutsTotal	Total number of LLDP frames that timed out in the cache.
LLDP FramesDiscardedTotal	Total number of LLDP frames that were discarded when any of the mandatory TLVs is missing, out of order, or contains out of range string length.
LLDP FramesInErrorsTotal	Total number of LLDP frames that were received with one or more detectable errors.
LLDP FramesInTotal	Total number of LLDP frames that the phone receives.
LLDP TLVDiscardedTotal	Total number of LLDP TLVs that are discarded.
LLDP TLVUnrecognizedTotal	Total number of LLDP TLVs that are not recognized on the phone.
CDP Neighbor Device ID	Identifier of a device connected to this port that CDP discovered.
CDP Neighbor IP Address	IP address of the neighbor device discovered that CDP protocol discovered.

Item	Description
CDP Neighbor Port	Neighbor device port to which the phone is connected discovered by CDP protocol.
LLDP Neighbor Device ID	Identifier of a device connected to this port discovered by LLDP discovered.
LLDP Neighbor IP Address	IP address of the neighbor device that LLDP protocol discovered.
LLDP Neighbor Port	Neighbor device port to which the phone connects that LLDP protocol discovered.
Port Information	Speed and duplex information.

## Device Logs

The following device log hyperlinks on a phone web page provide information that helps to monitor and troubleshoot the phone. To access a device log area, access the web page for the phone as described in [Access Web Page for phone, on page 155](#).

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

## Streaming Statistics

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

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

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

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

**Table 25: Streaming Statistics area items**

Item	Description
Remote Address	IP address and UDP port of the destination of the stream.
Local Address	IP address and UPD port of the phone.

Item	Description
Start Time	Internal time stamp indicates when Cisco Unified Communications Manager requested that the phone start transmitting packets.
Stream Status	Indication of whether streaming is active or not.
Host Name	Unique, fixed name that is automatically assigned to the phone based on the MAC address.
Sender Packets	Total number of RTP data packets that the phone transmitted since it started this connection. The value is 0 if the connection is set to receive-only mode.
Sender Octets	Total number of payload octets that the phone transmitted in RTP data packets since it started this connection. The value is 0 if the connection is set to receive-only mode.
Sender Codec	Type of audio encoding that is for the transmitted stream.
Sender Reports Sent (see note)	Number of times the RTCP Sender Report has been sent.
Sender Report Time Sent (see note)	Internal time-stamp indication as to when the last RTCP Sender Report was sent.
Rcvr Lost Packets	Total number of RTP data packets that have been lost since data reception started on this connection. Defined as the number of expected packets less the number of packets actually received, where the number of received packets includes any that are late or are duplicates. The value displays as 0 if the connection was set to send-only mode.
Avg Jitter	Estimate of mean deviation of the RTP data packet interarrival time, measured in milliseconds. The value displays as 0 if the connection was set to send-only mode.
Rcvr Codec	Type of audio encoding that is used for the received stream.
Rcvr Reports Sent (see note)	Number of times the RTCP Receiver Reports have been sent.
Rcvr Report Time Sent (see note)	Internal time-stamp indication as to when a RTCP Receiver Report was sent.
Rcvr Packets	Total number of RTP data packets that the phone has received since data reception started on this connection. Includes packets that were received from different sources if this call is a multicast call. The value displays as 0 if the connection was set to send-only mode.

Item	Description
Rcvr Octets	Total number of payload octets that the device received in RTP data packets since reception started on the connection. Includes packets that were received from different sources if this call is a multicast call. The value displays as 0 if the connection was set to send-only mode.
Cumulative Conceal Ratio	Total number of concealment frames divided by total number of speech frames that were received from the start of the voice stream.
Interval Conceal Ratio	Ratio of concealment frames to speech frames in the preceding 3-second interval of active speech. If voice activity detection (VAD) is in use, a longer interval might be required to accumulate three seconds of active speech.
Max Conceal Ratio	Highest interval concealment ratio from the start of the voice stream.
MOS LQK	Score that is an objective estimate of the mean opinion score (MOS) for listening quality (LQK) that rates from 5 (excellent) to 1 (bad). This score is based on audible concealment events that are to frame loss in the preceding eight-second interval of the voice stream. For more information, see <a href="#">Voice quality monitoring, on page 192</a> .  <b>Note</b> The MOS LQK score can vary due to the codec type that the Cisco IP Phone uses.
Avg MOS LQK	Average MOS LQK score that was observed for the entire voice stream.
Min MOS LQK	Lowest MOS LQK score that was observed from the start of the voice stream.
Max MOS LQK	Baseline or highest MOS LQK score that was observed from start of the voice stream.  These codecs provide the following maximum MOS LQK score under normal conditions with no frame loss: <ul style="list-style-type: none"> <li>• G.711 yields 4.5.</li> <li>• G.729 A /AB yields 3.7.</li> </ul>
MOS LQK Version	Version of the Cisco proprietary algorithm that is used to calculate MOS LQK scores.
Conceal Secs	Number of seconds that have concealment events (lost frames) from the start of the voice stream (includes severely concealed seconds).
Severely Conceal Secs	Number of seconds that have more than five percent concealment events (lost frames) from the start of the voice stream.
Latency (see note)	Estimate of the network latency, expressed in milliseconds. Represents a running average of the round-trip delay, measured when RTCP receiver report blocks are received.
Max Jitter	Maximum value of instantaneous jitter, in milliseconds.

Item	Description
Sender Size	RTP packet size, in milliseconds, for the transmitted stream.
Sender Reports Received (see note)	Number of times RTCP Sender Reports have been received.
Sender Report Time Received (see note)	Most recent time when an RTCP Sender Report was received.
Rcvr Size	RTP packet size, in milliseconds, for the received stream.
Rcvr Discarded	RTP packets that were received from the network but were discarded from the jitter buffers.
Rcvr Reports Received (see note)	Number of times RTCP Receiver Reports have been received.
Rcvr Report Time Received (see note)	Most recent time when an RTCP Receiver Report was received.
<b>Voice Quality Metrics</b>	
Cumulative Conceal Ratio	Total number of concealment frames divided by total number of speech frames that were received from the start of the voice stream.
Interval Conceal Ratio	Ratio of concealment frames to speech frames in preceding three-second interval of active speech. If voice activity detection (VAD) is in use, a longer interval might be required to accumulate 3 seconds of active speech.
Max Conceal Ratio	Highest interval concealment ratio from start of the voice stream.
Conceal Secs	Number of seconds that have concealment events (lost frames) from the start of the voice stream (includes severely concealed seconds).
Severely Conceal Secs	Number of seconds that have more than five percent concealment events (lost frames) from the start of the voice stream.

**Note**

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







# CHAPTER 13

## Troubleshooting

- [General troubleshooting information, page 169](#)
- [Startup problems, page 171](#)
- [Cisco IP Phone reset problems, page 174](#)
- [Phone cannot connect to LAN, page 176](#)
- [Cisco IP Phone security problems, page 177](#)
- [Audio and video problems , page 181](#)
- [General telephone call problems, page 182](#)
- [Troubleshooting procedures, page 183](#)
- [Additional troubleshooting information, page 188](#)

### General troubleshooting information

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

**Table 26: Cisco IP Phone troubleshooting**

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

Summary	Explanation
Moving a network connection from the phone to a workstation	<p>If you power your phone through the network connection, you must be careful if you decide to unplug the network connection of the phone and plug the cable into a desktop computer.</p> <p><b>Caution</b> The network card in the computer cannot receive power through the network connection; if power comes through the connection, the network card can be destroyed. To protect a network card, wait 10 seconds or longer after unplugging the cable from the phone before plugging it into a computer. This delay gives the switch enough time to recognize that there is no longer a phone on the line and to stop providing power to the cable.</p>
Changing the telephone configuration	<p>By default, the network configuration options are locked to prevent users from making changes that could impact their network connectivity. You must unlock the network configuration options before you can configure them. See <a href="#">Apply phone password, on page 36</a> for details.</p>
Codec mismatch between the phone and another device	<p>The RxType and the TxType statistics show the codec that is used for a conversation between this Cisco IP Phone and the other device. The values of these statistics should match. If they do not, verify that the other device can handle the codec conversation, or that a transcoder is in place to handle the service. See <a href="#">Display Call Statistics window</a> for details.</p>
Sound sample mismatch between the phone and another device	<p>The RxSize and the TxSize statistics show the size of the voice packets that are used in a conversation between this Cisco IP Phone and the other device. The values of these statistics should match. See <a href="#">Display Call Statistics window</a> for details.</p>
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 Configuration menu on the phone is set to 10 Half (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 appears in the switch console log:</p> <p>HALF_DUX_COLLISION_EXCEED_THRESHOLD</p> <p>To resolve this problem, reenabale the port from the switch.</p>

## Startup problems

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

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

### Related Topics

[Verify phone startup, on page 41](#)

## Cisco IP Phone does not go through 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

[Verify phone startup](#), on page 41

## 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 183 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 [Display Status Messages screen](#) for instructions about accessing status messages and for a list of potential errors, their explanations, and their solutions.

## Phone cannot connect to TFTP server or to Cisco Unified Communications Manager

### Problem

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

### Solution

Ensure that the network is currently running.

## 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 183](#)

**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 184](#)

**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 186](#)

**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 186](#).

## Configuration file corruption

### Problem

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

### Solution

Create a new phone configuration file. See [Create new phone configuration file, on page 185](#) for details.

## 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 48](#) 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 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 174](#) 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.

## Cisco IP Phone reset problems

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

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

## 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. See xref for more information. Verify that the DHCP server is set up properly. Verify the DHCP lease duration. Cisco recommends that you set it to 8 days.

## 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 Cisco Unified IP Phone appears to reset during heavy network usage, it is likely that you do not have a voice VLAN configured.

### Solution

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

## 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 **Admin Settings > Status > Network Statistics**.

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

## Phone resets due to DNS or other connectivity issues

### Problem

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

### Solution

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

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

## Cisco IP Phone security problems

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

### CTL file problems

The following sections describe troubleshooting problems with the CTL file.

#### Authentication error, phone cannot authenticate CTL file

**Problem**

A device authentication error occurs.

**Cause**

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

**Solution**

Install a correct certificate.

#### Phone cannot authenticate CTL file

**Problem**

Phone cannot authenticate the CTL file.

**Cause**

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

**Solution**

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

#### CTL file authenticates but other configuration files do not authenticate

**Problem**

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

**Cause**

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

**Solution**

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

**ITL file authenticates but other configuration files do not authenticate****Problem**

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

**Cause**

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

**Solution**

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

**TFTP authorization fails****Problem**

Phone reports TFTP authorization failure.

**Cause**

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

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

**Solution**

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

**Phone does not register****Problem**

Phone does not register with Cisco Unified Communications Manager.

**Cause**

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

**Solution**

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

## Signed configuration files are not requested

### Problem

Phone does not request signed configuration files.

### Cause

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

### Solution

Configure TFTP entries with certificates in the CTL file.

## 802.1X authentication problems

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

**Table 27: 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 Configuring IP or Registering.</li> <li>• 802.1X Authentication Status displays Held.</li> <li>• Status menu 802.1X status displays Failed.</li> </ul>	<p><a href="#">802.1X enabled on phone but phone does not authenticate, on page 180</a></p>
<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 Configuring IP or Registering.</li> <li>• 802.1X Authentication Status displays Disabled.</li> <li>• Status menu displays that the DHCP status has timed out.</li> </ul>	<p><a href="#">802.1X is not enabled, on page 180</a></p>

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 <code>Configuring IP</code> or <code>Registering</code>.</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 180</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 185](#).

### 802.1X is not enabled

#### Problem

The phone does not have 802.1X configured.

#### Cause

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

#### Solution

If 802.1X is not enabled on the phone, see [802.1X authentication, on page 82](#).

### Factory reset of phone has deleted 802.1X Shared Secret

#### Problem

After a reset, the phone does not authenticate.

**Cause**

These errors typically indicate that the phone has completed a factory reset (see xref) while 802.1X was enabled. A factory reset deletes the shared secret, which is required for 802.1X authentication and network access. See [Basic reset, on page 189](#).

**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, on page 82](#) for details.

## 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 audio

**Problem**

The recipient endpoint only sees a mute image.

**Solution**

If Auto Transmit Video is set to **Off**, the camera automatically transmits the mute image. The illuminated red LED on the top of the camera indicates that the video is muted. Set the Auto Transmit Video setting to **On** to restore video on the other side.

### 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.

## General telephone call problems

The following sections help troubleshoot general telephone call problems.

### Phone call cannot be established

**Problem**

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

**Cause**

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

**Solution**

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

## Phone does not recognize DTMF digits or digits are delayed

### Problem

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

### Cause

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

### Solution

Keys should not be pressed rapidly.

## Troubleshooting procedures

These procedures can be used to identify and correct problems.

### 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 **Admin 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 172](#)

### 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 Cisco Unified IP Phones use.
  - c) Assign a TFTP server. Use the same TFTP server that other functioning Cisco Unified IP Phones use.
- Step 3** On the Cisco Unified Communications Manager server, verify that the local host files have the correct Cisco Unified Communications Manager server name mapped to the correct IP address.
- Step 4** From Cisco Unified Communications Manager, choose **System > Server** and verify that reference to the server is made by the IP address and not by the DNS name.
- Step 5** From Cisco Unified Communications Manager, choose **Device > Phone**. Click **Find** to search for this phone. Verify that you have assigned the correct MAC address to this Cisco IP Phone.
- Step 6** Power cycle the phone.
- 

### Related Topics

- [Basic reset, on page 189](#)
- [Determine phone MAC address, on page 43](#)

## Check DHCP settings

### Procedure

---

- Step 1** On the Cisco Unified IP Phone, press **Applications**.
- Step 2** Select **Admin 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 173](#)



## Create new phone configuration file



### Note

- When you remove a phone from the Cisco Unified Communications Manager database, the configuration file is deleted from the Cisco Unified Communications Manager TFTP server. The phone directory number or numbers remain in the Cisco Unified Communications Manager database. They are called unassigned DNs and can be used for other devices. If unassigned DNs are not used by other devices, delete these DNs from the Cisco Unified Communications Manager database. You can use the Route Plan Report to view and delete unassigned reference numbers. See the *Cisco Unified Communications Manager Administration Guide* for more information.
- Changing the buttons on a phone button template, or assigning a different phone button template to a phone, may result in directory numbers that are no longer accessible from the phone. The directory numbers are still assigned to the phone in the Cisco Unified Communications Manager database, but the phone has no button on the phone with which calls can be answered. These directory numbers should be removed from the phone and deleted if necessary.

To create a new configuration file, follow these steps:

### Procedure

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

**Note** When you remove a phone from the Cisco Unified Communications Manager database, the configuration file is deleted from the Cisco Unified Communications Manager TFTP server. The phone directory number or numbers remain in the Cisco Unified Communications Manager database. They are called unassigned DNs and can be used for other devices. If unassigned DNs are not used by other devices, delete these DNs from the Cisco Unified Communications Manager database. You can use the Route Plan Report to view and delete unassigned reference numbers. See the *Cisco Unified Communications Manager Administration Guide* for more information.
- Step 3** Add the phone back to the Cisco Unified Communications Manager database.
- Step 4** Power cycle the phone.

### Related Topics

[Phone addition methods, on page 48](#)

## 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.

---

### Related Topics

[802.1X authentication, on page 82](#)

## Verify DNS settings

To verify DNS settings, follow these steps:

### Procedure

- 
- Step 1** Press **Applications**.
  - Step 2** Select **Admin 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 173](#)

## Start service




---

**Note** A service must be activated before it can be started or stopped.

---

To start a service, follow these steps:

### Procedure

- 
- Step 1** From Cisco Unified Communications Manager Administration, choose **Cisco Unified Serviceability** from the Navigation drop-down list and click **Go**.
  - Step 2** Choose **Tools > Control Center - Feature Services**.
  - Step 3** Choose the primary Cisco Unified Communications Manager server from the Server drop-down list. The window displays the service names for the server that you chose, the status of the services, and a service control panel to start or stop a service.
  - Step 4** If a service has stopped, click the corresponding radio button and then click **Start**.

The Service Status symbol changes from a square to an arrow.

---

## Troubleshoot using Debug menu

On the phone, the **Admin Settings > Debug Phone** menu enables you to troubleshoot phone problems.



### Note

When the debug level is set to Debug, the phone may experience degradation of service due to the amount of information that is collected. Use this level for the least amount of time necessary.

---

To debug a phone, you connect a computer to the PC port of the phone and start the debugging program. The computer requires a debugging program to be already installed. After changing the debug setting, the phone sends debug information to the debugging program on the computer.

For more information about debugging programs, contact Cisco TAC.

You can also connect to the phone using SSH (if enabled) to view the debug information. Limited debug information is available through the Phone web page, with the amount of information limited by the amount of available flash memory in the phone.

The debug setting persists when the phone restarts, resets, or power cycles. The debug settings reset when the phone is restored to the Factory Defaults, or when **Reset Settings > All** is selected.

### Before You Begin

- Computer with a phone debugging program installed.
- Cisco Unified Communications Manager must have the Settings Access parameter set to Enabled (default).
- Cisco Unified Communications Manager must have the Display Logging parameter set to PC Controlled (default) or Enabled.
  - PC Controlled means that the phone sends logs only when the debugging program is active on the computer and the computer is plugged into the PC port of the phone.
  - Enabled means that the logs are always sent to the PC port.

### Procedure

---

**Step 1** Access the debug information using one of the following methods:

- Connect a computer to the PC port of the phone that is experiencing problems. Launch the debugging program
- Connect to the phone using SSH (when enabled) to view the debug information.
- Check the phone web page. Note that the amount of information in the web page is limited by the amount of available flash memory on the phone.

**Step 2** On the phone that is experiencing problems, choose **Admin Settings > Debug Phone**.

**Step 3** Choose one of the following entries:

- **MMI** to troubleshoot user interface problems
- **Network** to troubleshoot network problems
- **CallControl** to troubleshoot problems with phone calls
- **Signaling** to troubleshoot communication problems
- **Security** to troubleshoot security problems

**Step 4** Choose one of the following debug levels:

- **Errors** to only log error messages. This setting is the phone default.
- **Warnings** to log error messages and warning messages.
- **Details** to log error and warning messages, as well as other details to assist troubleshooting.
- **Debug** to create a large amount of information, including error and warning messages.

**Step 5** Recreate the problem on the phone.

**Step 6** After you recreate the phone problem, navigate to **Admin Settings > Debug Phone** and set the debug level to **Errors**.

**Step 7** Use the captured debug information in the computer to diagnose the problem. For information on using the captured information, see the debugging program documentation.

---

## Additional troubleshooting information

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

<http://www.cisco.com/cisco/web/psa/troubleshoot.html>



# CHAPTER 14

## Maintenance

- [Basic reset, page 189](#)
- [Perform network configuration reset , page 191](#)
- [Perform user and network configuration reset, page 191](#)
- [Remove CTL file, page 191](#)
- [Quality Report Tool, page 192](#)
- [Voice quality monitoring, page 192](#)
- [Cisco IP Phone cleaning, page 194](#)

### Basic reset

Performing a basic reset of a Cisco 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 28: Basic reset methods**

Operation	Action	Explanation
Restart phone	Press <b>Services, Applications, or 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>Admin 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>Admin Settings &gt; Reset Settings &gt; Security</b> .	Resets the CTL file.

## Perform factory reset from phone keypad

Use these steps to reset the phone to factory default settings using the phone keypad.

### Procedure

---

- Step 1** Unplug the phone:
- If using PoE, unplug the LAN cable.
  - If using the power cube, unplug the power cube.
- Step 2** Wait 5 seconds.
- Step 3** Press and hold # and plug the phone back in.
- Step 4** When the light on the Mute button and handset light strip turns off and all other lights (Line button, Headset button, Speakerphone button and Select button) stay green, press **123456789\*0#** in sequence. When you press **1**, the lights on the line buttons turn red. The light on the Select button flashes when a button is pressed.

If you press the buttons out of sequence, the lights on the line button, headset button, speakerphone button, and Select button turn green. You need to start over and press **123456789\*0#** in sequence again.

After you press these buttons, the phone goes through the factory reset process.

**Caution** Do not power down the phone until it completes the factory reset process, and the main screen appears.

---

## Perform factory reset from phone menu

To perform a factory reset of a phone,

### Procedure

---

- Step 1** Press **Applications**.
- Step 2** Choose **Admin Settings > Reset Settings > All**.  
If required, unlock the phone options.
- 

### Related Topics

[Apply phone password, on page 36](#)

## 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 Admin Settings menu, if required, unlock phone options.
  - Step 2** Choose **Reset Settings > Network Settings**.
- 

### Related Topics

[Apply phone password, on page 36](#)

## Perform user and network configuration reset

Resets any user and network configuration changes that you have made, but that the phone has not written to flash memory, to previously saved settings.

### Procedure

---

- Step 1** From the Admin Settings menu, if required, unlock phone options.
  - Step 2** Choose **Reset Settings > Reset Device**.
- 

### Related Topics

[Apply phone password, on page 36](#)

## 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 Settings**.
- 

### Related Topics

[Apply phone password, on page 36](#)

## Quality Report Tool

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

You can configure user Cisco Unified IP Phones with QRT. When you do so, users can report problems with phone calls by pressing Report Quality. This softkey or button is available only when the Cisco Unified IP Phone is in the Connected, Connected Conference, Connected Transfer, or OnHook states.

When a user presses Report Quality, a list of problem categories appears. The user selects the appropriate problem category, and this feedback is logged in an XML file. Actual information that is logged depends on the user selection and whether the destination device is a Cisco Unified IP Phone.

For more information about using QRT, see *Cisco Unified Communications Manager Features and Services Guide*.

## Voice quality monitoring

To measure the voice quality of calls that are sent and received within the network, Cisco Unified IP Phones use 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.
- Mean Opinion Score (MOS) for Listening Quality (LQK) Voice Metrics: Uses a numeric score to estimate the relative voice-listening quality. The Cisco Unified IP Phones calculate the MOS LQK based audible-concealment events due to a frame loss in the preceding 8 seconds and includes weighting factors such as codec type and frame size.

MOS LQK scores are produced by a Cisco-proprietary algorithm, the Cisco Voice Transmission Quality (CVTQ) index. Depending on the MOS LQK version number, these scores may comply with the International Telecommunications Union (ITU) standard P.564. This standard defines evaluation methods and performance accuracy targets that predict listening quality scores based on observation of actual network impairment.



### Note

Concealment ratio and concealment seconds are primary measurements based on frame loss. A Conceal Ratio of zero indicates that the IP network is delivering frames and packets on time with no loss.

You can access voice quality metrics from the Cisco Unified IP Phone using the Call Statistics screen or remotely by using Streaming Statistics.

### Related Topics

[Call Statistics Screen](#)



## Voice quality troubleshooting tips

When you observe significant and persistent changes to metrics, use the following table for general troubleshooting information.

**Table 29: 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.

## 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 195
- [International Call Logging support](#), page 195

### 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 <http://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 “Locale installer” section in the *Cisco Unified Communications Operating System Administration Guide*.



**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.





## INDEX

### A

- alerts [17](#)
  - visual [17](#)
    - line state [17](#)
- Applications [17, 21, 25](#)
  - button [17, 21, 25](#)
    - Cisco Unified IP Phone 7821 [17](#)
    - Cisco Unified IP Phone 7841 [21](#)
    - Cisco Unified IP Phone 7861 [25](#)
- audible alert, See [alerts](#)

### B

- buttons [17, 21, 25](#)
  - Cisco Unified IP Phone 7821 [17](#)
    - Applications [17](#)
    - Conference [17](#)
    - Contacts [17](#)
    - Headset [17](#)
    - Hold [17](#)
    - line [17](#)
    - Messages [17](#)
    - Mute [17](#)
    - Navigation bar [17](#)
    - softkeys [17](#)
    - Speakerphone [17](#)
    - Transfer [17](#)
    - Volume [17](#)
  - Cisco Unified IP Phone 7841 [21](#)
    - Applications [21](#)
    - Conference [21](#)
    - Contacts [21](#)
    - Headset [21](#)
    - Hold [21](#)
    - Messages [21](#)
    - Mute [21](#)
    - Navigation bar [21](#)
    - programmable feature [21](#)
    - Select [21](#)
    - softkeys [21](#)

### buttons (continued)

- Cisco Unified IP Phone 7841 (continued)
  - Speakerphone [21](#)
  - Transfer [21](#)
  - Volume [21](#)
- Cisco Unified IP Phone 7861 [25](#)
  - Applications [25](#)
  - Conference [25](#)
  - Contacts [25](#)
  - Headset [25](#)
  - Hold [25](#)
  - Messages [25](#)
  - Mute [25](#)
  - Navigation bar [25](#)
  - programmable feature [25](#)
  - Select [25](#)
  - softkeys [25](#)
  - Speakerphone [25](#)
  - Transfer [25](#)
  - Volume [25](#)

### C

- Cisco Unified IP Phone 7821 [16, 17](#)
  - buttons and hardware [17](#)
  - connections [16](#)
  - screen [17](#)
    - location [17](#)
- Cisco Unified IP Phone 7841 [20, 21](#)
  - buttons and hardware [21](#)
  - connections [20](#)
  - screen [21](#)
    - location [21](#)
- Cisco Unified IP Phone 7861 [23, 25](#)
  - connections [23](#)
  - screen [25](#)
    - location [25](#)
- conference [17, 21, 25](#)
  - button [17, 21, 25](#)
    - Cisco Unified IP Phone 7821 [17](#)
    - Cisco Unified IP Phone 7841 [21](#)

- conference (*continued*)
  - button (*continued*)
    - Cisco Unified IP Phone 7861 [25](#)
- connections [16, 20, 23](#)
  - Cisco Unified IP Phone 7821 [16](#)
  - Cisco Unified IP Phone 7841 [20](#)
  - Cisco Unified IP Phone 7861 [23](#)
- contacts [17, 21, 25](#)
  - button [17, 21, 25](#)
    - Cisco Unified IP Phone 7821 [17](#)
    - Cisco Unified IP Phone 7841 [21](#)
    - Cisco Unified IP Phone 7861 [25](#)

## F

- flashing, See [alerts](#)

## H

- handset [17, 21, 25](#)
  - Cisco Unified IP Phone 7821 [17](#)
    - light strip [17](#)
    - location [17](#)
  - Cisco Unified IP Phone 7841 [21](#)
    - light strip [21](#)
    - location [21](#)
  - Cisco Unified IP Phone 7861 [25](#)
    - light strip [25](#)
    - location [25](#)
- handset rest [71](#)
- hardware [17, 21, 25](#)
  - Cisco Unified IP Phone 7821 [17](#)
  - Cisco Unified IP Phone 7841 [21](#)
  - Cisco Unified IP Phone 7861 [25](#)
- Headset [17, 21, 25](#)
  - button [17, 21, 25](#)
    - Cisco Unified IP Phone 7821 [17](#)
    - Cisco Unified IP Phone 7841 [21](#)
    - Cisco Unified IP Phone 7861 [25](#)
- Hold [17, 21, 25](#)
  - button [17, 21, 25](#)
    - Cisco Unified IP Phone 7821 [17](#)
    - Cisco Unified IP Phone 7841 [21](#)
    - Cisco Unified IP Phone 7861 [25](#)

## K

- keypad [17, 21, 25](#)
  - Cisco Unified IP Phone 7821 [17](#)
  - Cisco Unified IP Phone 7841 [21](#)

- keypad (*continued*)
  - Cisco Unified IP Phone 7861 [25](#)

## L

- LED, See [lights](#)
- lights [17](#)
  - amber, flashing [17](#)
  - green [17](#)
    - flashing [17](#)
    - steady [17](#)
  - handset [17](#)
  - red [17](#)
    - flashing [17](#)
    - steady [17](#)
- line [17](#)
  - buttons, Cisco Unified IP Phone 7821 [17](#)

## M

- menu [21, 25](#)
  - Applications [21, 25](#)
  - Directories [21, 25](#)
- messages [17, 21, 25](#)
  - button [17, 21, 25](#)
    - Cisco Unified IP Phone 7821 [17](#)
    - Cisco Unified IP Phone 7841 [21](#)
    - Cisco Unified IP Phone 7861 [25](#)
- mute [17, 21, 25](#)
  - button [17, 21, 25](#)
    - Cisco Unified IP Phone 7821 [17](#)
    - Cisco Unified IP Phone 7841 [21](#)
    - Cisco Unified IP Phone 7861 [25](#)

## N

- Navigation bar [17, 21, 25](#)
  - Cisco Unified IP Phone 7821 [17](#)
  - Cisco Unified IP Phone 7841 [21](#)
  - Cisco Unified IP Phone 7861 [25](#)

## P

- programmable feature buttons [21, 25](#)
  - Cisco Unified IP Phone 7841 [21](#)
  - Cisco Unified IP Phone 7861 [25](#)

**R**

ringer volume minimum level [17, 21, 25](#)

**S**

screen [17, 21, 25](#)

    Cisco Unified IP Phone 7821 [17](#)

        location [17](#)

    Cisco Unified IP Phone 7841 [21](#)

        location [21](#)

    Cisco Unified IP Phone 7861 [25](#)

        location [25](#)

Select button, See [Navigation bar](#)

softkeys [17, 21, 25](#)

    Cisco Unified IP Phone 7821 [17](#)

    Cisco Unified IP Phone 7841 [21](#)

    Cisco Unified IP Phone 7861 [25](#)

Speakerphone [17, 21, 25](#)

    button [17, 21, 25](#)

        Cisco Unified IP Phone 7821 [17](#)

        Cisco Unified IP Phone 7841 [21](#)

        Cisco Unified IP Phone 7861 [25](#)

status [17](#)

    buttons [17](#)

**T**

Transfer [17, 21, 25](#)

    button [17, 21, 25](#)

        Cisco Unified IP Phone 7821 [17](#)

        Cisco Unified IP Phone 7841 [21](#)

        Cisco Unified IP Phone 7861 [25](#)

**U**

UnifiedCisco Unified IP Phone 7861 [25](#)

    buttons and hardware [25](#)

**V**

visual alert, See [alerts](#)

Volume [17, 21, 25](#)

    Cisco Unified IP Phone 7821 [17](#)

    Cisco Unified IP Phone 7841 [21](#)

    Cisco Unified IP Phone 7861 [25](#)

    ringer volume [17, 21, 25](#)

