Cisco IP Phone 7800 Series Administration Guide for Cisco Unified Communications Manager

First Published: 2015-05-05

Last Modified: 2025-05-29

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

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

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

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

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

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

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

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

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

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

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

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

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

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

© 2015–2023 Cisco Systems, Inc. All rights reserved.

CONTENTS

PREFACE

Preface xiii

Overview xiii

Audience xiii

Guide Conventions xiii

Related Documentation xiv

Cisco IP Phone 7800 Series Documentation xiv

Cisco Unified Communications Manager Documentation xv

Cisco Business Edition 6000 Documentation xv

Documentation, Support, and Security Guidelines xv

Cisco Product Security Overview xv

CHAPTER 1

New and Changed Information 1

New and Changed Information for Firmware Release 14.3(1)SR3 1

New and Changed Information for Firmware Release 14.2(1) 2

New and Changed Information for Firmware Release 14.1(1) 2

New and Changed Information for Firmware Release 14.0(1) 2

New and Changed Information for Firmware Release 12.8(1) 3

New and Changed Information for Firmware Release 12.7(1) 3

New and Changed Information for Firmware Release 12.6(1) 3

New Information for Firmware Release 12.5(1)SR3 3

New Information for Firmware Release 12.5(1)SR2 4

New Information for Firmware Release 12.5(1)SR1 4

New Information for Firmware Release 12.5(1) 4

New Information for Firmware Release 12.1(1)SR1 5

New Information for Firmware Release 12.1(1) 5

New and Changed Information for Firmware Release 12.0(1) 5

New Information for Firmware Release 11.7(1) 5
New Information for Firmware Release 11.5(1)SR1 6
New Information for Firmware Release 11.5(1) 6
New Information for Firmware Release 11.0 7

PART I About the Cisco IP Phone 9

CHAPTER 2 Technical Details 11
Physical and Operating Environment Specifications 11
Cable Specifications 12
Network and Computer Port Pinouts 12
Network Port Connector 13
Computer Port Connector 13
Phone Power Requirements 14
Power Outage 15
Power Reduction 15
Power Negotiation Over LLDP 15
Network Protocols 16
VLAN Interaction 19
Cisco Unified Communications Manager Interaction 19
Cisco Unified Communications Manager Express Interaction 20
External Devices 21
Phone Behavior During Times of Network Congestion 21
Application Programming Interface 21

CHAPTER 3 Cisco IP Phone Hardware 23
Cisco IP Phone Hardware Overview 23
Hardware Versions 25
Cisco IP Phone 7811 25
Phone Connections 25
Cisco IP Phone 7821 27
Phone Connections 27
Cisco IP Phone 7841 28
Phone Connections 28

Cisco IP Phone 7861 29
Phone Connections 29
Buttons and Hardware 30
Softkey, Line, and Feature Buttons 32
Terminology Differences 32

PART II **Cisco IP Phone Installation** 35

CHAPTER 4 **Cisco IP Phone Installation** 37
Verify the Network Setup 37
Activation Code Onboarding for On-premises Phones 38
Activation Code Onboarding and Mobile and Remote Access 39
Enable Autoregistration for Phones 39
Install the Cisco IP Phone 41
Share a Network Connection with Your Phone and Computer 42
Set Up the Phone from the Setup Menus 43
Apply a Phone Password 44
Text and Menu Entry From the Phone 44
Configure Network Settings 45
Network Setup 45
IPv4 Fields 47
IPv6 Fields 49
Verify Phone Startup 51
Configure Phone Services for Users 51
Change a User's Phone Model 52

CHAPTER 5 **Cisco Unified Communications Manager Phone Setup** 55
Set Up a Cisco IP Phone 55
Determine the Phone MAC Address 60
Phone Addition Methods 60
Add Phones Individually 60
Add Phones with a BAT Phone Template 61
Add Users to Cisco Unified Communications Manager 62
Add a User from an External LDAP Directory 62

Add a User Directly to Cisco Unified Communications Manager 63
Add a User to an End User Group 63
Associate Phones with Users 64
Surviveable Remote Site Telephony 65

CHAPTER 6 Self Care Portal Management 69
Self Care Portal Overview 69
Set Up User Access to the Self Care Portal 69
Customize the Self Care Portal Display 70

PART III Cisco IP Phone Administration 71

CHAPTER 7 Cisco IP Phone Security 73
Cisco IP Phone Security Overview 73
Security Enhancements for Your Phone Network 74
View the Current Security Features on the Phone 75
View Security Profiles 76
Supported Security Features 76
Set Up a Locally Significant Certificate 78
Enable FIPS Mode 79
Phone Call Security 79
Secure Conference Call Identification 80
Secure Phone Call Identification 81
802.1x Authentication 82

CHAPTER 8 Cisco IP Phone Customization 85
Custom Phone Ringtones 85
Set Up Wideband Codec 85
Set Up Handset for 7811 86
Set Up Idle Display 86
Customize the Dial Tone 87

CHAPTER 9 Phone Features and Setup 89
Cisco IP Phone User Support 89

Telephone Features 89
Feature Buttons and Softkeys 106
Phone Feature Configuration 108
Set Up Phone Features for All Phones 108
Set Up Phone Features for a Group of Phones 109
Set Up Phone Features for a Single Phone 109
Product Specific Configuration 109
Feature Configuration Best Practices 123
High Call Volume Environments 123
Multiline Environments 123
Field: Always Use Prime Line 124
Disable Transport Layer Security Ciphers 124
Enable Call History for Shared Line 125
Schedule Power Save for Cisco IP Phone 125
Schedule EnergyWise on Cisco IP Phone 127
Set up AS-SIP 130
Set Up Do Not Disturb 132
Enable Agent Greeting 132
Set Up Monitoring and Recording 133
Set Up Call Forward Notification 134
Enable BLF for Call Lists 135
Enable Device Invoked Recording 135
UCR 2008 Setup 136
Set Up UCR 2008 in Common Device Configuration 136
Set Up UCR 2008 in Common Phone Profile 137
Set Up UCR 2008 in Enterprise Phone Configuration 137
Set Up UCR 2008 in Phone 138
Set Up RTP/sRTP Port Range 138
Mobile and Remote Access Through Expressway 139
Deployment Scenarios 140
Media Paths and Interactive Connectivity Establishment 140
Phone Features Available for Mobile and Remote Access Through Expressway 141
Problem Report Tool 143
Configure a Customer Support Upload URL 143

Set the Label for a Line 145
Assured Services SIP 145
Multilevel Precedence and Preemption 146
Migration of your Phone to a Multiplatform Phone Directly 146
Set Up Softkey Template 146
Phone Button Templates 149
Modify Phone Button Template 149
Set Up PAB or Speed Dial as IP Phone Service 149
Headset Management on Older Versions of Cisco Unified Communications Manager 151
Download the Default Headset Configuration File 151
Modify the Default Headset Configuration File 152
Install the Default Configuration File on Cisco Unified Communications Manager 154
Restart the Cisco TFTP Server 154

CHAPTER 10 **Corporate and Personal Directory Setup** 157
Corporate Directory Setup 157
Personal Directory Setup 157
User Personal Directory Entries Setup 158
Download Cisco IP Phone Address Book Synchronizer 158
Cisco IP Phone Address Book Synchronizer Deployment 159
Install Synchronizer 159
Set Up Synchronizer 159

PART IV **Cisco IP Phone Troubleshooting** 161

CHAPTER 11 **Monitoring Phone Systems** 163
Monitoring Phone Systems Overview 163
Cisco IP Phone Status 163
Display the Phone Information Window 164
Display Status Menu 164
Display Status Messages Window 164
Display Network Information Screen 169
Display Network Statistics Window 170
Display Call Statistics Window 173

Display Security Setup Window 175
Cisco IP Phone Web Page 176
Access the Phone Web Page 176
Device Information 176
Network Setup 178
Network Statistics 184
Device Logs 187
Streaming Statistics 187
Request Information from the Phone in XML 189
Sample CallInfo Output 190
Sample LineInfo Output 190
Sample ModeInfo Output 191

CHAPTER 12 Troubleshooting 193
General Troubleshooting Information 193
Startup Problems 194
Cisco IP Phone Does Not Go Through the Normal Startup Process 195
Cisco IP Phone Does Not Register with Cisco Unified Communications Manager 196
Phone Displays Error Messages 196
Phone Cannot Connect to TFTP Server or to Cisco Unified Communications Manager 196
Phone Cannot Connect to TFTP Server 196
Phone Cannot Connect to Server 197
Phone Cannot Connect Using DNS 197
Cisco Unified Communications Manager and TFTP Services Are Not Running 197
Configuration File Corruption 197
Cisco Unified Communications Manager Phone Registration 198
Cisco IP Phone Cannot Obtain IP Address 198
Phone Reset Problems 198
Phone Resets Due to Intermittent Network Outages 199
Phone Resets Due to DHCP Setting Errors 199
Phone Resets Due to Incorrect Static IP Address 199
Phone Resets During Heavy Network Usage 199
Phone Resets Due to Intentional Reset 200
Phone Resets Due to DNS or Other Connectivity Issues 200

Phone Does Not Power Up 200
Phone Cannot Connect to LAN 200
Cisco IP Phone Security Problems 201
CTL File Problems 201
Authentication Error, Phone Cannot Authenticate CTL File 201
Phone Cannot Authenticate CTL File 201
CTL File Authenticates but Other Configuration Files Do Not Authenticate 201
ITL File Authenticates but Other Configuration Files Do Not Authenticate 202
TFTP Authorization Fails 202
Phone Does Not Register 202
Signed Configuration Files Are Not Requested 203
Audio Problems 203
No Speech Path 203
Choppy Speech 203
Troubleshooting Procedures 203
Create a Phone Problem Report from Cisco Unified Communications Manager 204
Create a Console Log from Your Phone 204
Check TFTP Settings 204
Determine DNS or Connectivity Issues 205
Check DHCP Settings 205
Create a New Phone Configuration File 206
Verify DNS Settings 207
Start Service 207
Control Debug Information from Cisco Unified Communications Manager 208
Additional Troubleshooting Information 209

CHAPTER 13 **Maintenance** 211
Basic Reset 211
Factory Reset the Phone with the Keypad 211
Perform Reset All Settings from Phone Menu 212
Perform Factory Reset from Phone Menu 212
Perform Custom Reset from Phone Menu 213
Reboot Your Phone from the Backup Image 213
Remove CTL File 213

Voice Quality Monitoring 214
Voice Quality Troubleshooting Tips 214
Cisco IP Phone Cleaning 215

CHAPTER 14 International User Support 217
Unified Communications Manager Endpoints Locale Installer 217
International Call Logging Support 217
Language Limitation 218

Preface

- Overview, on page xiii
- Audience, on page xiii
- Guide Conventions, on page xiii
- Related Documentation, on page xiv
- Documentation, Support, and Security Guidelines, on page xv

Overview

Cisco IP Phone 7800 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
boldface font	Commands and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[]	Elements in square brackets are optional.

Convention	Description
{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 w include the quotation marks.
`screen` font	Terminal sessions and information the system displays are in `screen` font.
`input` font	Information you must enter is in **`input`** font.
italic screen font	Arguments for which you supply values are in *italic screen* font.
^	The symbol ^ represents the key labeled Control - for example, the key combination ^D in a s 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

Find documentation specific to your language, phone model, and call control system on the product support page for the Cisco IP Phone 7800 Series.

Cisco Unified Communications Manager Documentation

See the *Cisco Unified Communications Manager Documentation Guide* and other publications that are specific to your Cisco Unified Communications Manager release on the product support page.

Cisco 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:

https://www.cisco.com/c/en/us/support/unified-communications/business-edition-6000/tsd-products-support-series-home.html

Documentation, Support, and Security Guidelines

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

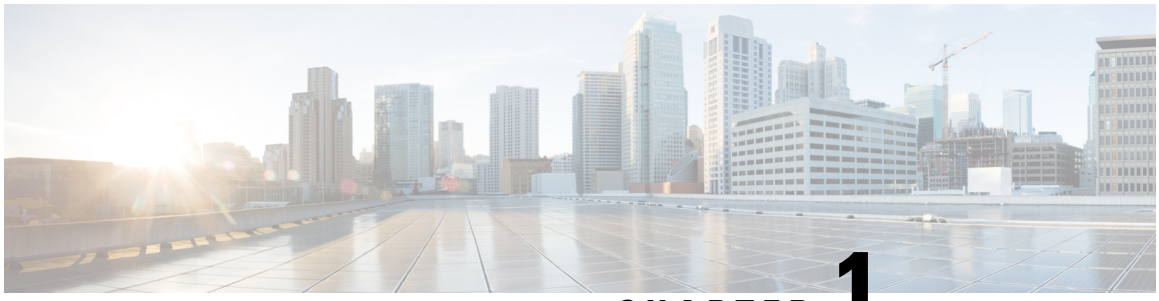
http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

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

Cisco Product Security Overview

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

Further information regarding U.S. export regulations can be found at https://www.bis.gov/ear.



CHAPTER 1

New and Changed Information

- New and Changed Information for Firmware Release 14.3(1)SR3, on page 1
- New and Changed Information for Firmware Release 14.2(1), on page 2
- New and Changed Information for Firmware Release 14.1(1), on page 2
- New and Changed Information for Firmware Release 14.0(1), on page 2
- New and Changed Information for Firmware Release 12.8(1), on page 3
- New and Changed Information for Firmware Release 12.7(1), on page 3
- New and Changed Information for Firmware Release 12.6(1), on page 3
- New Information for Firmware Release 12.5(1)SR3, on page 3
- New Information for Firmware Release 12.5(1)SR2, on page 4
- New Information for Firmware Release 12.5(1)SR1, on page 4
- New Information for Firmware Release 12.5(1), on page 4
- New Information for Firmware Release 12.1(1)SR1, on page 5
- New Information for Firmware Release 12.1(1), on page 5
- New and Changed Information for Firmware Release 12.0(1), on page 5
- New Information for Firmware Release 11.7(1), on page 5
- New Information for Firmware Release 11.5(1)SR1, on page 6
- New Information for Firmware Release 11.5(1), on page 6
- New Information for Firmware Release 11.0, on page 7

New and Changed Information for Firmware Release 14.3(1)SR3

The following information is new or changed for Firmware Release 14.3(1)SR3.

Feature	New or Changed
Added the new parameter "TLS Client Min Version". Updated the default value of the parameter "Disable TLS 1.0 and TLS 1.1 for Web Access" from "Disabled" to "Enabled".	Product Specific Configuration, on page 109

New and Changed Information for Firmware Release 14.2(1)

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

Feature	New or Changed
Support for SIP OAuth on SRST	Security Enhancements for Your Phone Network, on page 74
New settings for Cisco Headset 500 Series: Dock Event and Always On Mode	Telephone Features, on page 89

New and Changed Information for Firmware Release 14.1(1)

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

Feature	New or Changed
SIP OAuth for Proxy TFTP support	Security Enhancements for Your Phone Network, on page 74
Configurable Delayed PLAR	Telephone Features, on page 89
MRA Support for Extension Mobility Login with Cisco Headsets	Telephone Features, on page 89
Phone Migration without Transition Load	Migration of your Phone to a Multiplatform Phone Directly, on page 146

New and Changed Information for Firmware Release 14.0(1)

Table 1: New and Changed Information

Feature	New or Changed
User Interface Enhancements	Surviveable Remote Site Telephony, on page 65 Telephone Features, on page 89
SIP OAuth Enhancements	Security Enhancements for Your Phone Network, on page 74
OAuth Enhancements for MRA	Mobile and Remote Access Through Expressway, on page 139

As of Firmware Release 14.0, the phones support DTLS 1.2. DTLS 1.2 requires Cisco Adaptive Security Appliance (ASA) Release 9.10 or later. You configure the minimum DTLS version for a VPN connection in ASA. For more information, see *ASDM Book 3: Cisco ASA Series VPN ASDM Configuration Guide* at

https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html

New and Changed Information for Firmware Release 12.8(1)

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

Feature	New or Changed Content
Phone Data Migration	Change a User's Phone Model, on page 52
Headset Update Enhancement	Device Information, on page 176
Simplify Extension Mobility Login with Cisco Headsets	Telephone Features, on page 89
Add additional information about the Web Access field	Product Specific Configuration, on page 109
Remove an unsupported feature from the table	Telephone Features, on page 89

New and Changed Information for Firmware Release 12.7(1)

Table 2: Cisco IP Phone 7800 Administration Guide Revisions for Firmware Release 12.7(1)

Revision	Updated Section
Cisco Headset 500 Series Firmware Release 2.0	• New section: Headset Management on Older Versions of Cisco Unified Communications Manager, on page 151 • Device Information, on page 176
Updated for incoming hunt group calls.	Telephone Features, on page 89
E-hook configuration information was removed.	Product Specific Configuration, on page 109

New and Changed Information for Firmware Release 12.6(1)

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

New Information for Firmware Release 12.5(1)SR3

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

Table 3: Cisco IP Phone 7800 Administration Guide Revisions for Firmware Release 12.5(1)SR3

Revision	Updated Section
Support for Activation Code Onboarding and Mobile and Remote Access	Activation Code Onboarding and Mobile and Remote Access, on page 39
Support for Problem Report Tool use from Cisco Unified Communications Manager.	Create a Phone Problem Report from Cisco Unified Communications Manager, on page 204
New topic	Share a Network Connection with Your Phone and Computer, on page 42

New Information for Firmware Release 12.5(1)SR2

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

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

New Information for Firmware Release 12.5(1)SR1

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

Table 4: Cisco IP Phone 7800 Administration Guide Revisions for Firmware Release 12.5(1)SR1

Revision	Updated Section
Support for Elliptic Curve support	Supported Security Features, on page 76
Support for Media Paths and Interactive Connectivity Establishment	Media Paths and Interactive Connectivity Establishment, on page 140
Support for Activation Code Onboarding	Activation Code Onboarding for On-premises Phones, on page 38
Support for Remote Configuration of Headset Parameters	Headset Management on Older Versions of Cisco Unified Communications Manager, on page 151

New Information for Firmware Release 12.5(1)

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

Table 5: Cisco IP Phone 7800 Administration Guide Revisions for Firmware Release 12.5(1)

Revision	Updated Section
Support for Whisper Paging on Cisco Unified Communications Manager Express	Cisco Unified Communications Manager Express Interaction, on page 20
Support for Disable TLS Ciphers	Product Specific Configuration, on page 109
Support for Disable handset	Product Specific Configuration, on page 109

New Information for Firmware Release 12.1(1)SR1

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

Table 6: Cisco IP Phone 7800 Administration Guide Revisions for Firmware Release 12.1(1)SR1

Revision	Updated Section
Enbloc Dialing for Inter-Digit Timer T.302 Enhancement.	Product Specific Configuration, on page 109

New Information for Firmware Release 12.1(1)

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

Table 7: Cisco IP Phone 7800 Administration Guide Revisions for Firmware Release 12.1(1)

Revision	Updated Section
Enabling or disabling TLS 1.2 for web server access is now supported.	Product Specific Configuration, on page 109
The G722.2 AMR-WB audio codec is now supported.	Cisco IP Phone Hardware Overview, on page 23
	Call Statistics Fields, on page 173

New and Changed Information for Firmware Release 12.0(1)

No updates were required for firmware release 12.0(1).

New Information for Firmware Release 11.7(1)

No administration updates were required for firmware release 11.7(1).

New Information for Firmware Release 11.5(1)SR1

All new features have been added to Telephone Features, on page 89.

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

Table 8: Cisco IP Phone 7800 Administration Guide Revisions for Firmware Release 11.5(1)SR1

Revision	Updated Section
General	New presentation of phone feature configuration in Cisco Unified Communications Manager Phone Feature Configuration, on page 108
Updated for Configurable Ringer support	Product Specific Configuration, on page 109
Updated for Do not disturb with MLPP support	Set up AS-SIP, on page 130
Enhanced Security	Security Enhancements for Your Phone Network, on page 74

New Information for Firmware Release 11.5(1)

All new features have been added to Telephone Features, on page 89.

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

Table 9: Cisco IP Phone 7800 Administration Guide Revisions for Firmware Release 11.5(1).

Revision	Updated Section
Enhanced Security	Security Enhancements for Your Phone Network, on page 74
Updated for Opus codec	Cisco IP Phone Hardware Overview, on page 23
Updated for FIPS	Enable FIPS Mode, on page 79 Status Messages Fields, on page 164
Added Disable Recents softkey	Product Specific Configuration, on page 109
Added Customize Dial Tone	Customize the Dial Tone, on page 87
Added Display Network Info Screen	Display Network Information Screen, on page 169

New Information for Firmware Release 11.0

All new features have been added to Telephone Features, on page 89.

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

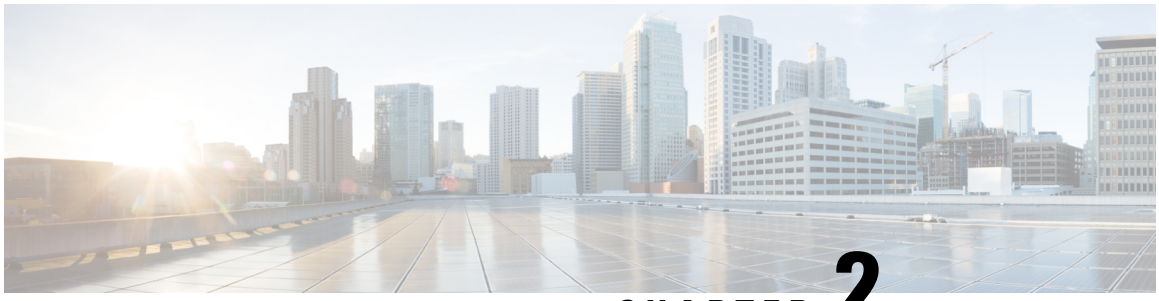
Table 10: Cisco IP Phone 7800 Administration Guide Revisions for Firmware Release 11.0.

Revision	Updated Section
Updated these sections for improved cBarge support	Telephone Features, on page 89 Feature Buttons and Softkeys, on page 106
Updated these section for improved Problem Report Tool(PRT) support:	Problem Report Tool, on page 143. Configure a Customer Support Upload URL, on page 143
Added for Line Text Label	Set the Label for a Line, on page 145.

PART I

About the Cisco IP Phone

- Technical Details, on page 11
- Cisco IP Phone Hardware, on page 23



CHAPTER 2

Technical Details

- Physical and Operating Environment Specifications, on page 11
- Cable Specifications, on page 12
- Network and Computer Port Pinouts, on page 12
- Phone Power Requirements, on page 14
- Network Protocols, on page 16
- VLAN Interaction, on page 19
- Cisco Unified Communications Manager Interaction, on page 19
- Cisco Unified Communications Manager Express Interaction, on page 20
- External Devices, on page 21
- Phone Behavior During Times of Network Congestion, on page 21
- Application Programming Interface, on page 21

Physical and Operating Environment Specifications

The following table shows the physical and operating environment specifications for the Cisco IP Phone 7800 Series.

Table 11: Physical and Operating Specifications

Specification	Value or Range
Operating temperature	32° to 104°F (0° to 40°C)
Operating relative humidity	10% to 90% (noncondensing)
Storage temperature	14° to 140°F (–10° to 60°C)
Height	8.14 in. (207 mm)
Width	• Cisco IP Phone 7811— 7.67 in. (195 mm) • Cisco IP Phone 7821 — 8.11 in. (206 mm) • Cisco IP Phone 7841 — 8.11 in. (206 mm) • Cisco IP Phone 7861— 10.42 in. (264.91 mm)

Specification	Value or Range
Depth	1.1 in. (28 mm)
Weight	• Cisco IP Phone 7811— 0.84 kg • Cisco IP Phone 7821 — 0.867 kg • Cisco IP Phone 7841 — 0.868 kg • Cisco IP Phone 7861— 1.053 kg
Power	• 100-240 VAC, 50-60 Hz, 0.5 A—When using the AC adapter • 48 VDC, 0.2 A—When using the in-line power over the network
Cables	Cisco IP Phone 7811, 7821, 7841, and 7861: • Category 3/5/5e/6 for 10-Mbps cables with 4 pairs • Category 5/5e/6 for 100-Mbps cables with 4 pairs Cisco IP Phone 7841: Category 5/5e/6 for 1000-Mbps cables with 4 pa **Note** 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 max (330feet).

Cable Specifications

- RJ-9 jack (4-conductor) for handset and headset connection.

Note The Cisco IP Phone 7811 does not contain a headset jack.

- RJ-45 jack for the LAN 10/100BaseT connection (on Cisco IP Phones 7811, 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 7811, 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:

Network Port Connector

The following table describes the network port connector pinouts.

Table 12: Network Port Connector Pinouts

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

Computer Port Connector

The following table describes the computer port connector pinouts.

Table 13: 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-

Pin Number	Function
Note 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 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.

Table 14: Guidelines for Cisco IP Phone Power

Power Type	Guidelines
External power: Provided through the CP-PWR-CUBE-3= external power supply	The Cisco IP Phone uses the CP-PWR-CUBE-3 power supply.
External power—Provided through the Cisco IP Phone Power Injector	The Cisco IP Phone Power Injector may be used with most Cisco IP Phones. The phone identifies if the phone can use the power injector. Functioning as a midspan device, the injector delivers inline power to the attached ph Cisco IP Phone Power Injector connects between a switch port and the IP Phone, and 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.	To ensure uninterruptible operation of the phone, make sure that the switch has a back supply. Make sure that the CatOS or IOS version that runs on your switch supports your intend deployment. See the documentation for your switch for operating system version inf

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

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

Document topics	URL
PoE Solutions	http://www.cisco.com/c/en/us/solutions/enterprise-networks/power-over-ethernet-solutions/index.html
Cisco Catalyst Switches	http://www.cisco.com/c/en/us/products/switches/index.html

Document topics	URL
Integrated Service Routers	http://www.cisco.com/c/en/us/products/routers/index.html
Cisco IOS Software	http://www.cisco.com/c/en/us/products/ios-nx-os-software/inc

Power Outage

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

Power Reduction

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

Power Save

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

Note The Cisco IP Phone 7811 does not support Power Save because the phone screen does not have a backlight.

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.

Note The Cisco IP Phone 7811 does not support Power Save Plus.

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.

Power Negotiation Over LLDP

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

After a phone reboots, the switch locks to one protocol (CDP or LLDP) for power negotiation. The switch locks to the first protocol (containing a power Threshold Limit Value [TLV]) that the phone transmits. If the

system administrator disables that protocol on the phone, the phone cannot power up any accessories because the switch does not respond to power requests in the other protocol.

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

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

Note

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

Network Protocols

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

Table 15: Supported Network Protocols on the Cisco IPPhone

Network Protocol	Purpose
Bootstrap Protocol (BootP)	BootP enables a network device, such as the Cisco IP Phone, to disco certain startup information, such as its IP address.
Cisco Audio Session Tunneling (CAST)	The CAST protocol allows IP phones and associated applications beh phone to discover and communicate with the remote endpoints witho requiring changes to the traditional signaling components like Cisco U Communications Manager and gateways. The CAST protocol allows se hardware devices to synchronize related media and it allows PC applic to augment nonvideo-capable phones to become video enabled using as the video resource.
Cisco Discovery Protocol (CDP)	CDP is a device-discovery protocol that runs on all Cisco-manufactu equipment. A device can use CDP to advertise its existence to other devices and r information about other devices in the network.
Domain Name Server (DNS)	DNS translates domain names to IP addresses.

Network Protocol	Purpose
Dynamic Host Configuration Protocol (DHCP)	DHCP dynamically allocates and assigns an IP address to networ DHCP enables you to connect an IP phone into the network and h phone become operational without the need to manually assign an or to configure additional network parameters.
Hypertext Transfer Protocol (HTTP)	HTTP is the standard protocol for transfer of information and mo documents across the Internet and the web.
Hypertext Transfer Protocol Secure (HTTPS)	Hypertext Transfer Protocol Secure (HTTPS) is a combination of Hypertext Transfer Protocol with the SSL/TLS protocol to provide and secure identification of servers. **Note** IP phones can be HTTPS clients; they cannot be HTTPS servers.
IEEE 802.1X	The IEEE 802.1X standard defines a client-server-based access c authentication protocol that restricts unauthorized clients from con a LAN through publicly accessible ports. Until the client is authenticated, 802.1X access control allows only Authentication Protocol over LAN (EAPOL) traffic through the po the client is connected. After authentication is successful, normal pass through the port.
Internet Protocol (IP)	IP is a messaging protocol that addresses and sends packets acros network.
Link Layer Discovery Protocol (LLDP)	LLDP is a standardized network discovery protocol (similar to C supported on some Cisco and third-party devices.

Network Protocol	Purpose
Link Layer Discovery Protocol-Media Endpoint Devices (LLDP-MED)	LLDP-MED is an extension of the LLDP standard developed for voi products.
Network Transport Protocol (NTP)	NTP is a networking protocol for clock synchronization between con systems over packet-switched, variable-latency data networks.
Real-Time Transport Protocol (RTP)	RTP is a standard protocol for transporting real-time data, such as inte voice and video, over data networks.
Real-Time Control Protocol (RTCP)	RTCP works in conjunction with RTP to provide QoS data (such as j latency, and round trip delay) on RTP streams.
Session Initiation Protocol (SIP)	SIP is the Internet Engineering Task Force (IETF) standard for multi conferencing over IP. SIP is an ASCII-based application-layer control p (defined in RFC 3261) that can be used to establish, maintain, and ter calls between two or more endpoints.
Secure Real-Time Transfer protocol (SRTP)	SRTP is an extension of the Real-Time Protocol (RTP) Audio/Video and ensures the integrity of RTP and Real-Time Control Protocol (RT packets providing authentication, integrity, and encryption of media p between two endpoints.
Transmission Control Protocol (TCP)	TCP is a connection-oriented transport protocol.
Transport Layer Security (TLS)	TLS is a standard protocol for securing and authenticating communic
Trivial File Transfer Protocol (TFTP)	TFTP allows you to transfer files over the network. On the Cisco IPPhone, TFTP enables you to obtain a configuration fi specific to the phone type.
User Datagram Protocol (UDP)	UDP is a connectionless messaging protocol for delivery of data pac

Related Topics

Cisco Unified Communications Manager Documentation, on page xv
Verify Network Setup , on page 37
Verify Phone Startup , on page 51

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

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

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

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

Related Topics

Cisco Unified Communications Manager Documentation, on page xv

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 or Hold softkey.

Barge

Not supported.

Direct Transfer

Not supported.

Select

Not supported.

Users cannot create conference and transfer calls across different lines.

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

External Devices

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

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

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

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

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

Phone Behavior During Times of Network Congestion

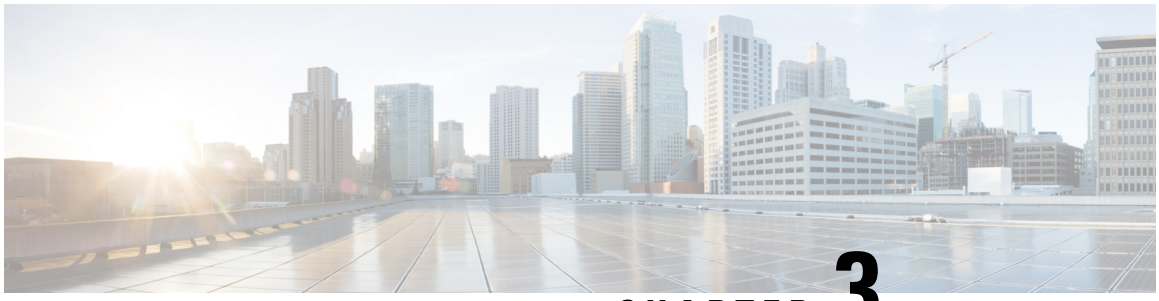
Anything that degrades network performance can affect phone audio and, in some cases, can cause a call to drop. Sources of network degradation can include, but are not limited to, the following activities:

- Administrative tasks, such as an internal port scan or security scan.
- Attacks that occur on your network, such as a Denial of Service attack.

Application Programming Interface

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

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



CHAPTER 3

Cisco IP Phone Hardware

- Cisco IP Phone Hardware Overview, on page 23
- Hardware Versions, on page 25
- Cisco IP Phone 7811, on page 25
- Cisco IP Phone 7821, on page 27
- Cisco IP Phone 7841, on page 28
- Cisco IP Phone 7861, on page 29
- Buttons and Hardware, on page 30
- Terminology Differences, on page 32

Cisco IP Phone Hardware Overview

The Cisco IP Phone 7800 Series provides voice communication over an Internet Protocol (IP) network. The CiscoIPPhone 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 Phone 7841 supports Gigabit ethernet connectivity.

When adding features to the phone line keys, you are limited by the number of line keys available. You cannot add more features than the number of line keys on your phone.

Table 16: Cisco IP Phone 7800 Series and Supported Line Keys

Phone	Supported Line Keys
Cisco IP Phone 7811	0
Cisco IP Phone 7821	2
Cisco IP Phone 7841	4
Cisco IP Phone 7861	16

A Cisco IP Phone, like other network devices, must be configured and managed. These phones encode the following codecs:

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

These phones decode the following codecs:

- G.711 a-law
- G.711 mu-law
- G.722
- G.729
- G.729a
- G.729b
- G.729ab
- iLBC
- Opus

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

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

Cisco IP Phones can interact with other services and devices on your IP network to provide enhanced functionality. For example, you can integrate Cisco Unified Communications Manager with the corporate Lightweight Directory Access Protocol 3 (LDAP3) standard directory to enable users to search for coworker contact information directly from their IP phones. You can also use XML to enable users to access information such as weather, stocks, quote of the day, and other web-based information.

Hardware Versions

We occasionally update our phone hardware to take advantage of new technology, with each version identified by a Product ID (PID) located on the back of your phone. Use the following table to determine if your phone is an early hardware release or a later one.

New phones must run Firmware Release 10.3(1) or later and you cannot downgrade to an earlier firmware release.

Table 17: Cisco IP Phone 7800 Series Hardware Versions

Cisco IP Phone	Original Hardware Version	Current Hardware Version
Cisco IP Phone 7811	-	CP-7811-K9=V01
Cisco IP Phone 7821	CP-7821-K9=V01	CP-7821-K9=V03
Cisco IP Phone 7841	CP-7841-K9=V01, V02, or V03	CP-7841-K9=V04 or later
Cisco IP Phone 7861	CP-7861-K9=V02	CP-7861-K9=V03 or later

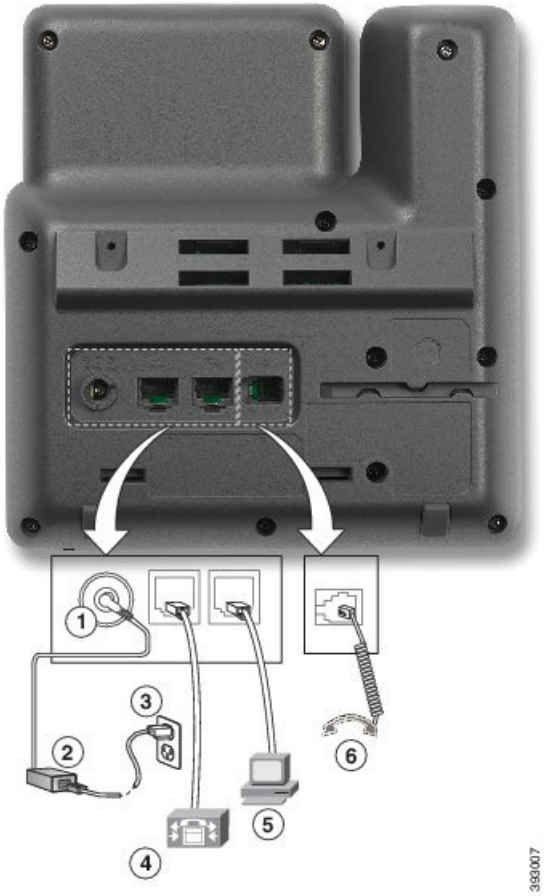
Related Topics

Factory Reset the Phone with the Keypad, on page 211

Cisco IP Phone 7811

Phone Connections

Use an Ethernet cable to connect your phone to your LAN and enable the phone's full functionality. If your Ethernet port is equipped with Power over Ethernet (PoE), you can power the phone through the LAN port. Do not extend the LAN Ethernet cable outside the building. For your phone to work, it must be connected to the IP telephony network.



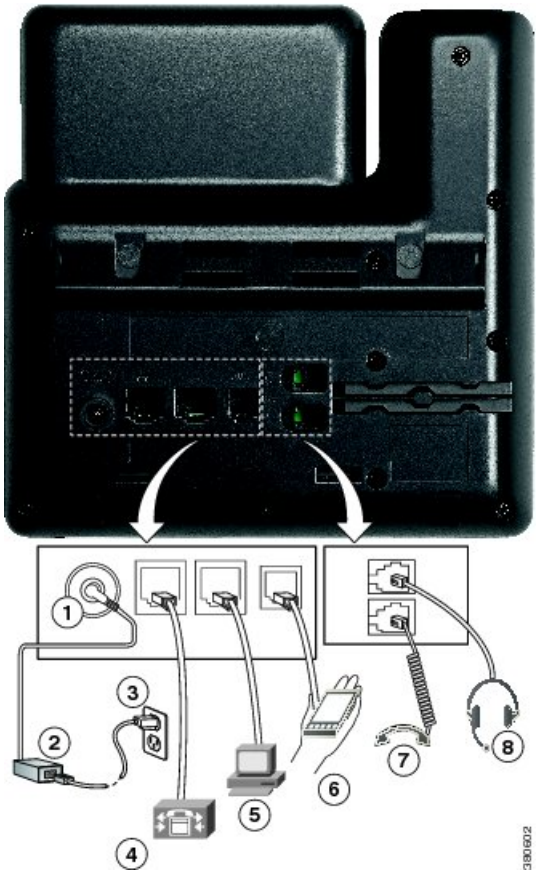
1	DC adapter port (DC48V).	4	Network port (10/100 SW) connection. IEEE 802.3af power enabled.
2	AC-to-DC power supply (optional).	5	Access port (10/100 PC) connection (optional).
3	AC power wall plug (optional).	6	Handset connection.

Note In the EU and UK, your phone is shipped with a power switch cable that is required in order to provide power to your phone when using an AC-to-DC power supply. Connect the power cord to the power switch cable and then connect the other end of the power switch cable to the DC adapter port.

Cisco IP Phone 7821

Phone Connections

Connect your Cisco IP phone to your LAN with an Ethernet cable to enable full functionality of your Cisco IP phone. If your Ethernet port is equipped with Power over Ethernet (PoE), you can power the Cisco IP phone through the LAN port. Do not extend the LAN Ethernet cable outside the building. For your phone to work, it must be connected to the IP telephony network.



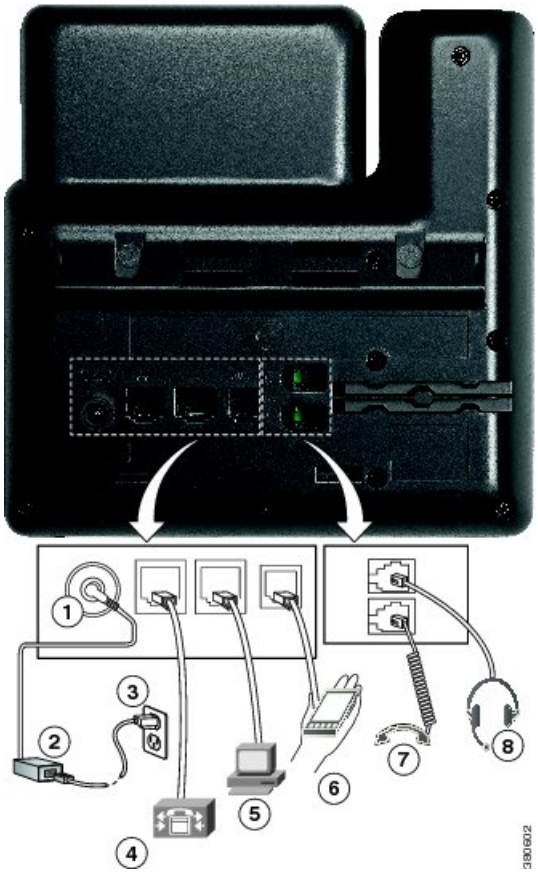
1	DC adaptor port (DC48V) (optional).	5	Access port (10/100 PC) connection (optional).
2	AC-to-DC power supply (optional).	6	Auxiliary port (optional).
3	AC power wall plug (optional).	7	Handset connection.
4	Network port (10/100 SW) connection. IEEE 802.3af power enabled.	8	Analog headset connection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

Note In the EU and UK, your phone is shipped with a power switch cable that is required in order to provide power to your phone when using an AC-to-DC power supply. Connect the power cord to the power switch cable and then connect the other end of the power switch cable to the DC adapter port.

Cisco IP Phone 7841

Phone Connections

Connect your Cisco IP phone to your LAN with an Ethernet cable to enable full functionality of your Cisco IP phone. If your Ethernet port is equipped with Power over Ethernet (PoE), you can power the Cisco IP phone through the LAN port. Do not extend the LAN Ethernet cable outside the building. For your phone to work, it must be connected to the IP telephony network.



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

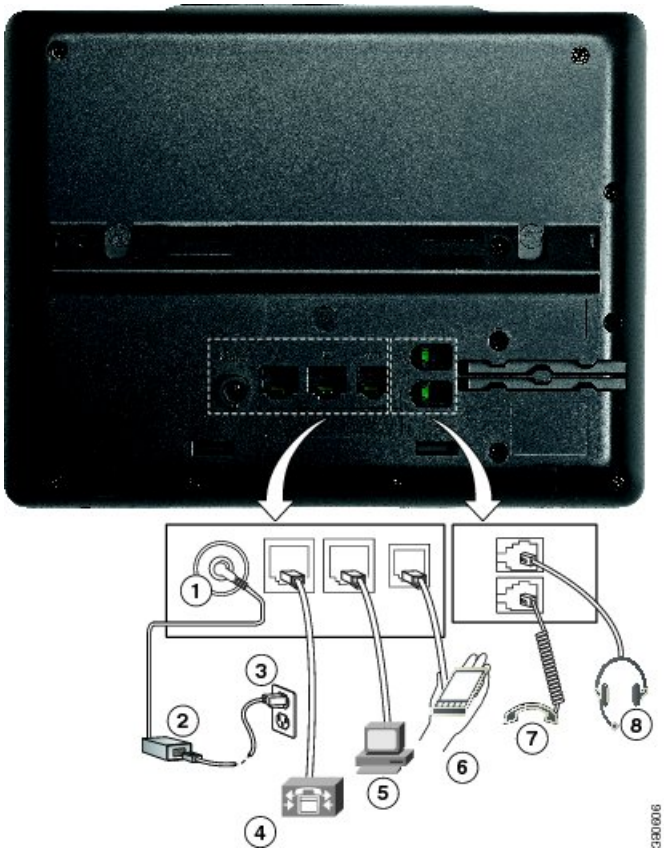
3	AC power wall plug (optional).	7	Handset connection.
4	Network port (10/100/1000 SW) connection. IEEE 802.3af power enabled.	8	Analog headset connection (optional).

Note In the EU and UK, your phone is shipped with a power switch cable that is required in order to provide power to your phone when using an AC-to-DC power supply. Connect the power cord to the power switch cable and then connect the other end of the power switch cable to the DC adapter port.

Cisco IP Phone 7861

Phone Connections

Connect your Cisco IP phone to your LAN with an Ethernet cable to enable full functionality of your Cisco IP phone. If your Ethernet port is equipped with Power over Ethernet (PoE), you can power the Cisco IP phone through the LAN port. Do not extend the LAN Ethernet cable outside the building. For your phone to work, it must be connected to the IP telephony network.



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

Note In the EU and UK, your phone is shipped with a power switch cable that is required in order to provide power to your phone when using an AC-to-DC power supply. Connect the power cord to the power switch cable and then connect the other end of the power switch cable to the DC adapter port.

Buttons and Hardware

The Cisco IP Phone 7800 Series has distinct hardware types:

- Cisco IP Phone 7811 No buttons on either side of the screen
- Cisco IP Phone 7821 Two buttons on the left side of the screen
- Cisco IP Phone 7841 Two buttons on either side of the screen
- Cisco IP Phone 7861 16 buttons at the right edge of the phone

Figure 1: Cisco IP Phone 7800 Series Buttons and Features

The following table describes the Cisco IP Phone 7800 Series buttons and hardware.

Table 18: Cisco IP Phone 7800 Series Buttons and Features

1	Handset and Handset light strip	Indicates whether you have an incoming call (flashing red) or a new voice message (steady red).
2	Programmable feature buttons and line buttons	Access your phone lines, features, and call sessions. For more information, see Softkey, Line, and Feature Buttons, on page 32. The Cisco IP Phone 7811 does not have programmable feature buttons or line buttons.
3	Softkey buttons	Access functions and services. For more information, see Softkey, Line, and Feature Buttons, on page 32.
4	Navigation cluster	Navigation ring and **Select** button. Scroll through menus, highlight items, and select the highlighted item.
5	**Hold/Resume**, **Conference**, and **Transfer**	**Hold/Resume** Place an active call on hold and resume the held call. **Conference** Create a conference call. **Transfer** Transfer a call.
6	**Speakerphone**, **Mute**, and **Headset**	**Speakerphone** Toggle the speakerphone on or off. When the speakerphone is on, the button is lit. **Mute** Toggle the microphone on or off. When the microphone is muted, the button is lit. **Headset** Toggle the headset on. When the headset is on, the button islit. To leave headset mode, you pick up the handset or select **Speakerphone**. The Cisco IP Phone 7811 does not have a **Headset** button.
7	**Contacts**, **Applications**, and **Messages**	**Contacts** Access personal and corporate directories. **Applications** Access call history, user preferences, phone settings, and phone model information. **Messages** Autodial your voice messaging system.
8	**Volume** button	Adjust the handset, headset, and speakerphone volume (off hook) and the ringer volume(on hook).

Softkey, Line, and Feature Buttons

You can interact with the features on your phone in several ways:

- Softkeys, located below the screen, give you access to the function displayed on the screen above the softkey. The softkeys change depending on what you are doing at the time. The **More ...** softkey shows you that more functions are available.
- Feature and line buttons, located on either side of the screen, give you access to phone features and phone lines.
  - Feature buttons—Used for features such as **Speed dial** or **Call pickup**, and to view your status on another line.
  - Line buttons—Used to answer a call or resume a held call. When not used for an active call, used to initiate phone functions, such as the missed calls display.

Feature and line buttons illuminate to indicate status.

- Green, steady LED—Active call or two-way intercom call
- Green, flashing LED—Held call
- Amber, steady LED—Privacy in use, one-way intercom call, or logged into a Hunt Group
- Amber, flashing LED—Incoming call or reverting call
- Red, steady LED—Remote line in use (shared line or Line Status) or Do Not Disturb (DND) active
- Red, flashing LED—Remote line on hold

Your administrator can set up some functions as softkeys or as feature buttons. You can also access some functions with softkeys or the associated hard button.

Terminology Differences

The following table highlights some of the terminology differences in the *Cisco IP Phone 7800 Series User Guide*, the *Cisco IP Phone 7800 Series Administration Guide for Cisco Unified Communications Manager* , and the Cisco Unified Communications Manager documentation.

Table 19: Terminology Differences

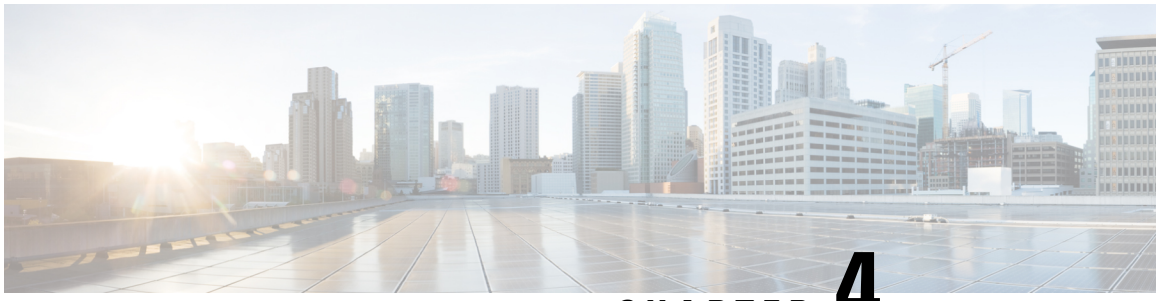
User Guide	Administration Guide
Line Status	Busy Lamp Field (BLF)
Message Indicators	Message Waiting Indicator (MWI) or Message Waiting Lamp
Programmable Feature Button	Programmable Button or Programmable Line Key (PLK)

User Guide	Administration Guide
Voicemail System	Voice Messaging System

PART II

Cisco IP Phone Installation

- Cisco IP Phone Installation, on page 37
- Cisco Unified Communications Manager Phone Setup, on page 55
- Self Care Portal Management, on page 69



CHAPTER 4

Cisco IP Phone Installation

- Verify the Network Setup, on page 37
- Activation Code Onboarding for On-premises Phones, on page 38
- Activation Code Onboarding and Mobile and Remote Access, on page 39
- Enable Autoregistration for Phones, on page 39
- Install the Cisco IP Phone, on page 41
- Set Up the Phone from the Setup Menus, on page 43
- Configure Network Settings, on page 45
- Verify Phone Startup, on page 51
- Configure Phone Services for Users, on page 51
- Change a User's Phone Model, on page 52

Verify the Network Setup

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

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

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

Procedure

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

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

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

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

Related Topics

Cisco Unified Communications Manager Documentation, on page xv

Activation Code Onboarding for On-premises Phones

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

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

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

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

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

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

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

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

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

Activation Code Onboarding and Mobile and Remote Access

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

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

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

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

For more information, see the following documents:

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

Enable Autoregistration for Phones

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

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

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

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

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

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

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

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

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

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

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

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

Procedure

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

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

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

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

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

Step 5 Click **Save**.

Step 6 Click **Apply Config**.

Related Topics

Cisco Unified Communications Manager Documentation, on page xv

Install the Cisco IP Phone

After the phone connects to the network, the phone startup process begins, and the phone registers with CiscoUnified 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 21.

If you only have one LAN cable at your desk, you can plug your phone into the LAN with the SW port and then connect your computer into the PC port. For more information, see Share a Network Connection with Your Phone and Computer, on page 42.

You can also daisy chain two phones together. Connect the PC port of the first phone to the SW port of the second phone.

Caution Do not connect the SW and PC ports into the LAN.

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 14.

Step 2 Connect the handset to the handset port and press the cable into the cable channel.

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.

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

Step 3 Connect a headset to the headset port and press the cable into the cable channel. You can add a headset later if you do not connect one now.

Note
The Cisco IP Phone 7811 does not have a headset port.

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

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.

Note
The Cisco IP Phone 7811 does not support a headset.

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, 5e, or 6 cabling for 10 Mbps connections; Category 5, 5e, or 6 for 100Mbps connections; and Category 5e or 6 for 1000 Mbps connections. For more information, see Network and Computer Port Pinouts, on page 12.

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.

Use Category 3, 5, 5e, or 6 cabling for 10 Mbps connections; Category 5, 5e, or 6 for 100Mbps connections; and Category 5e or 6 for 1000 Mbps connections. For more information, see Network and Computer Port Pinouts, on page 12 for guidelines.

Step 7 If the phone is on a desk, adjust the footstand. With a wall-mounted phone, you might need to adjust the handset rest to ensure that the receiver cannot slip out of the cradle.

Note
You cannot adjust the Cisco IP Phone 7811 footstand.

Step 8 Monitor the phone startup process. This step 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.

Step 10 Upgrade the phone to the current firmware image.

Step 11 Make calls with the Cisco IP Phone to verify that the phone and features work correctly.

See the *Cisco IP Phone 7800 Series User Guide*.

Step 12 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 IPPhones.

Share a Network Connection with Your Phone and Computer

Both your phone and your computer must connect to your network to function. If you only have one Ethernet port, then your devices can share the network connection.

Before you begin

Your administrator must enable the PC port in Cisco Unified Communications Manager before you can use it.

Procedure

Step 1 Connect the phone SW port to the LAN with an Ethernet cable.

Step 2 Connect your computer to the phone PC port with an Ethernet cable.

Set Up the Phone from the Setup Menus

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

The phone includes the following setup menus:

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

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

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

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

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

Procedure

Step 1 Press **Applications** .

Step 2 Select **Admin Settings**.

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

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

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

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

Step 6 To display a submenu, repeat step 5.

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

Apply a Phone Password

You can apply a password to the phone. If you do, 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 (**Device** > **Device Settings** > **Common Phone Profile**).

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

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

Text and Menu Entry From the Phone

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

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

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

Configure Network Settings

Procedure

Step 1 Press **Applications** .

Step 2 To access the Network Settings menu, select **Admin settings** > **Network Setup**.

Step 3 Set the fields as described in .

Step 4 After you have set the fields, select **Apply** and **Save**.

Step 5 Reboot the phone.

Network Setup

The Network Setup menu contains fields and submenus for IPv4 and IPv6. To change some of the fields, first disable DHCP.

Table 20: Ethernet Setup Menu Options

Entry	Type	Default	Description
IPv4 setup	Menu		See the IPv4 Fields section. This option displays only when the phone is configured in IPv4-only mode or in IPv4 and IPv6 mode.
IPv6 setup	Menu		See the “IPv6 Fields” section.
Host Name	String		Host name that the DHCP server assigned to the phone.
Domain Name	String		Name of the Domain Name System (DNS) domain in which the phone resides. To change this field, turn off DHCP.
Operational VLAN ID			Auxiliary Virtual Local Area Network (VLAN) configured on a Cisco Catalyst switch of which the phone is a member. This setting is blank if the auxiliary VLAN or the Administrative VLAN are configured. If the phone has not received an auxiliary VLAN, this option indicates the Administrative VLAN. The phone doesn't inherit the Operational VLAN from Admin VLAN if Cisco Discovery Protocol or Link Level Discovery Protocol Media Endpoint Discovery is enabled. To assign a VLAN ID manually, use the Admin VLAN ID option.

Entry	Type	Default	Description
Admin VLAN ID			Auxiliary VLAN of which the phone is a member. Used only if the phone does not receive an auxiliary VLAN from the switch; otherwise, this value is ignored.
PC VLAN			Allows the phone to interoperate with third-party switches that do not support a voice VLAN. The Admin VLAN ID option must be set before you can change this option.
SW Port Setup	Auto Negotiate 1000 Full 100 Half 10 Half 10 Full	Auto Negotiate	Speed and duplex of the network port. Valid values specify: • Auto Negotiate • 1000 Full:1000-BaseT/full duplex • 100 Half: 100-BaseT/half duplex • 100 Full: 100-BaseT/full duplex • 10 Half: 10-BaseT/half duplex • 10 Full: 10-BaseT/full duplex If the phone is connected to a switch, configure the switch port to the same speed as the phone, or configure both to autonegotiate. Unlock network configuration options if you want to edit this setting. If you change the setting of this option, you must change the PC Port Configuration option to the same setting.
PC Port Setup	Auto Negotiate 1000 Full 100 Half 10 Half 10 Full	Auto Negotiate	Speed and duplex of the Computer (access) port. Valid values: • Auto Negotiate • 1000 Full: 1000-BaseT/full duplex • 100 Half: 100-BaseT/half duplex • 100 Full: 100-BaseT/full duplex • 10 Half: 10-BaseT/half duplex • 10 Full: 10-BaseT/full duplex If the phone is connected to a switch, configure the port on the switch to the same speed as the phone, or configure both to autonegotiate. Unlock network configuration options if you want to change this field. If you change the setting, you must change the SW Port Configuration option to the same setting. To configure the setting on multiple phones simultaneously, enable Remote Port Configuration in the Enterprise Phone Configuration window (**System** > **Enterprise Phone Configuration**). If the ports are configured for Remote Port Configuration in Cisco Unified Communications Manager Administration, the data cannot be changed on the phone.
UDP-MED			

IPv4 Fields

Table 21: IPv4 Setup Menu Options

Entry	Type	Default	Description
DHCP Enabled			Indicates whether the phone has DHCP enabled or disabled. When DHCP is enabled, the DHCP server assigns the phone an IP address. When DHCP is disabled, the administrator must manually assign an IP address to the phone.
IP Address			Internet Protocol (IP) address of the phone. If you assign an IP address with this option, you must also assign a subnet mask and default router. See the Subnet Mask and Default Router options in this table.
Subnet Mask			Subnet mask used by the phone.
Default Router			Default router used by the phone.
DNS Server 1			Primary Domain Name System (DNS) server (DNS Server 1) that the phone uses.
Alternate TFTP			Indicates whether the phone is using an alternate TFTP server.

Entry	Type	Default	Description
TFTP Server 1			Primary Trivial File Transfer Protocol (TFTP) server that the phone uses. If you are not using DHCP in your network and you want to change this server, you must use the TFTP Server 1 option. If you set the Alternate TFTP option to On, you must enter a nonzero value for the TFTP Server 1 option. If neither the primary TFTP server nor the backup TFTP server is listed in the CTL or ITL file on the phone, you must unlock the file before you can save changes to the TFTP Server 1 option. In this case, the phone deletes the file when you save changes to the TFTP Server 1 option. A new CTL or ITL file downloads from the new TFTP Server 1 address. When the phone looks for the TFTP server, the phone gives precedence to manually assigned TFTP servers, regardless of the protocol. If your configuration includes both IPv6 and IPv4 TFTP servers, the phone prioritizes the order that it looks for the TFTP server by giving priority to manually assigned IPv6 TFTP servers and IPv4 TFTP servers. The phone looks for the TFTP server in this order: **1.** Any manually assigned IPv4 TFTP servers **2.** Any manually assigned IPv6 servers **3.** DHCP assigned TFTP servers **4.** DHCPv6 assigned TFTP servers **Note** For information about the CTL and ITL files, see the *Cisco Unified Communications Manager Security Guide*.

Entry	Type	Default	Description
TFTP Server 2			Optional backup TFTP server that the phone uses if the primary TFTP server is unavailable. If neither the primary TFTP server nor the backup TFTP server is listed in the CTL or ITL file on the phone, you must unlock either of the files before you can save changes to the TFTP Server 2 option. In this case, the phone deletes either of the files when you save changes to the TFTP Server 2 option. A new CTL or ITL file downloads from the new TFTP Server 2 address. If you forget to unlock the CTL or ITL file, you can change the TFTP Server 2 address in either file, then erase them by pressing Erase from the Security Configuration menu. A new CTL or ITL file downloads from the new TFTP Server 2 address. When the phone looks for the TFTP server, it gives precedence to manually assigned TFTP servers, regardless of the protocol. If your configuration includes both IPv6 and IPv4 TFTP servers, the phone prioritizes the order that it looks for the TFTP server by giving priority to manually assigned IPv6 TFTP servers and IPv4 TFTP servers. The phone looks for the TFTP server in the following order: **1.** Any manually assigned IPv4 TFTP servers **2.** Any manually assigned IPv6 servers **3.** DHCP assigned TFTP servers **4.** DHCPv6 assigned TFTP servers **Note** For information about the CTL or ITL file, see Cisco Unified Communications Manager Security Guide.
DHCP Address Released			Releases the IP address that DHCP assigned. This field is editable if DHCP is enabled. If you wish to remove the phone from the VLAN and release the IP address for reassignment, set this option to Yes and press Apply.

IPv6 Fields

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

- IP Addressing Mode
- IP Addressing Mode Preference for Signalling

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

For more details about IPv6 deployment, see the IPv6 Deployment Guide for Cisco Collaboration Systems Release 12.0.

You set up IPv6 from one of the following menus:

- When Wi-Fi is disabled: **Ethernet Setup** > **IPv6 setup**
- When Wi-Fi is enabled: **Wi-Fi Client Setup** > **IPv6 setup**

Use the phone keypad to enter or edit an IPv6 address. To enter a colon, press the asterisk (*) on the keypad. To enter hexadecimal digits a, b, and c, press 2 on the keypad, scroll to select the required digit, and press **Enter**. To enter hexadecimal digits d, e, and f, press 3 on the keypad, scroll to select the required digit, and press **Enter**.

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

Table 22: IPv6 Setup Menu Options

ue	pEntry	Descriptiony	T
	DHCPv6 Enabled	Indicates the method that the phone uses to get the IPv6-only address. When DHCPv6 is enabled, the phone gets the IPv6 address either from DHCPv6 server or from SLAAC by RA sent by the IPv6-enabled router. And if DHCPv6 is disabled, the phone will not have any stateful (from DHCPv6 server) or stateless (from SLAAC) IPv6 address.	
	IPv6 Address	Displays the current IPv6-only address of the phone or allows the user to enter a new IPv6 address. A valid IPv6 address is 128 bits in length, including the subnet prefix. Two address formats are supported: • Eight sets of hexadecimal digits separated by colons X:X:X:X:X:X:X:X • Compressed format to collapse a single run of consecutive zero groups into a single group represented by a double colon. If the IP address is assigned with this option, you must also assign the IPv6 prefix length and the default router.	
	IPv6 Prefix Length	Displays the current prefix length for the subnet or allows the user to enter a new prefix length. The subnet prefix length is a decimal value from 1 to 128.	
	IPv6 Default Router	Displays the default router used by the phone or allows the user to enter a new IPv6-only default router.	
	IPv6 DNS Server 1	Displays the primary DNSv6 server used by the phone or allows the user to enter a new server.	
	IPv6 Alternate TFTP	Allows the user to enable the use of an alternate (secondary) IPv6 TFTP server.	
	IPv6 TFTP Server 1	Displays the primary IPv6 TFTP server used by the phone or allows the user to set a new primary TFTP server.	
	IPv6 TFTP Server 2	(Optional) Displays the secondary IPv6 TFTP server used if the primary IPv6 TFTP server is unavailable or allows the user to set a new secondary TFTP server.	
	IPv6 Address Release	Allows the user to release IPv6-related information.	

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 you are using Power over Ethernet, plug the LAN cable into the Network port.

Step 2 If you are 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.

Note
For Cisco IP Phone 8861, if you are using a power cube but there is no Power over Ethernet available, then the wifi will be enabled.

Related Topics

Startup Problems, on page 194
Cisco IP Phone Does Not Go Through the Normal Startup Process, on page 195

Configure Phone Services for Users

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

Before a user can access any service:

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

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

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

Procedure

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

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

See Self Care Portal Overview, on page 69 for a summary of the information that you must provide to end users.

Related Topics

Cisco Unified Communications Manager Documentation, on page xv

Change a User's Phone Model

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

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

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

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

The phone reboots when the configuration is complete.

Before you begin

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

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

Procedure

Step 1 Power off the old phone.

Step 2 Power on the new phone.

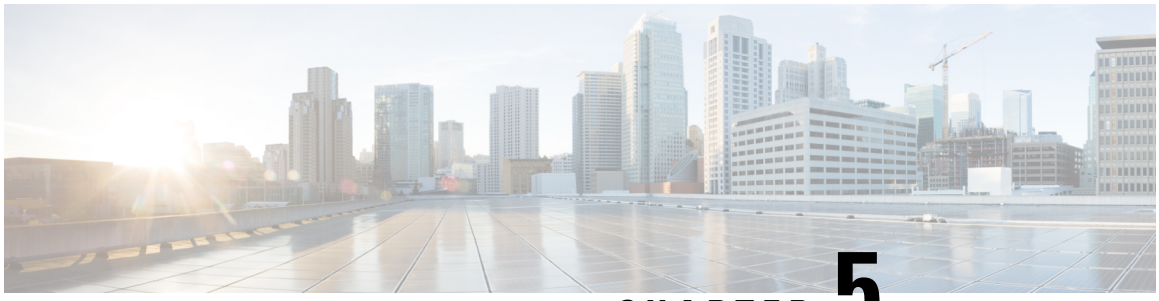
Step 3 On the new phone, select **Replace an existing phone**.

Step 4 Enter the primary extension of the old phone.

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

Step 6 Press **Submit**.

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



CHAPTER 5

Cisco Unified Communications Manager Phone Setup

- Set Up a Cisco IP Phone, on page 55
- Determine the Phone MAC Address, on page 60
- Phone Addition Methods, on page 60
- Add Users to Cisco Unified Communications Manager, on page 62
- Add a User to an End User Group, on page 63
- Associate Phones with Users , on page 64
- Surviveable Remote Site Telephony, on page 65

Set Up a Cisco IP Phone

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

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

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

Procedure

Step 1 Gather the following information about the phone:

- Phone model
- MAC address: see Determine the Phone MAC Address, on page 60
- 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 the phone button template, softkey template, phone features, IP Phone services, or phone applications

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

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

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

Step 3 Define the 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 documentation for your particular Cisco Unified Communications Manager release and the related links.

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.

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.

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.

Step 7 Configure a security profile for the device type and protocol. Select **System** > **Security** > **Phone Security Profile**.

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 the documentation for your particular Cisco Unified Communications Manager release.

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

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

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

Step 9 Select **Device** > **Device Settings** > **SIP Profile** to set up parameters such as Multilevel Precedence and Preemption (MLPP).

Step 10 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 about directory numbers, see the documentation for your particular Cisco Unified Communications Manager release and the related links.

Step 11 Associate the user with a phone. Click **Associate End Users** at the bottom of the Phone Configuration window to associate a user to the line that is being configured.

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

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

c) Select **Save**.

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

d) If the phone has a second line, configure Line 2.

Step 12 Associate the user with the device:

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

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

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

Step 13 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.

Step 14 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 15 Configure Cisco IPPhone services and assign services. Select **Device** > **Device Settings** > **Phone Services**.

Provides IP Phone services to the phone.

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

Step 16 (Optional) Assign services to programmable buttons. Select **Device** > **Device Settings** > **Phone button template**.

Provides access to an IP phone service or URL.

Step 17 Add user information to the global directory for Cisco UnifiedCommunications Manager. Select **User Management** > **End User**, and then click **Add New** and configure the required fields. Required fields are indicated by an asterisk (*).

Note
If your company uses a Lightweight Directory Access Protocol (LDAP) directory to store information on users, you can install and configure Cisco Unified Communications to use your existing LDAP directory, see Corporate Directory Setup, on page 157. After the Enable Synchronization from the LDAP Server field is enabled, you will not be able to add additional users from Cisco Unified Communications Manager Administration.

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

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

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

Step 18 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 a User to an End User Group, on page 63.

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

Related Topics

Cisco Unified Communications Manager Documentation, on page xv

Determine the Phone MAC Address

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

Procedure

Perform one of the following actions:

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

Phone Addition Methods

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

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

Before you add phones individually or with BAT, you need the MAC address of the phone. For more information, see Determine the Phone MAC Address, on page 60.

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

Related Topics

Cisco Unified Communications Manager Documentation, on page xv

Add Phones Individually

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

Procedure

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

Step 2 Click **Add New**.

Step 3 Select the phone type.

Step 4 Select **Next**.

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

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

Step 6 Select **Save**.

Related Topics

Cisco Unified Communications Manager Documentation, on page xv

Add Phones with a BAT Phone Template

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

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

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

Procedure

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

Step 2 Click **Add New**.

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

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

Step 5 Click **Save**.

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

Related Topics

Cisco Unified Communications Manager Documentation, on page xv

Add Users to Cisco Unified Communications Manager

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

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

Procedure

Step 1 To add users individually, see Add a User Directly to Cisco Unified Communications Manager, on page 63.

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

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

Related Topics

Cisco Unified Communications Manager Documentation, on page xv

Add a User from an External LDAP Directory

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

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

Procedure

Step 1 Sign into Cisco Unified Communications Manager Administration.

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

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

Step 4 Click on the LDAP directory name.

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

Add a User Directly to Cisco Unified Communications Manager

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

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

Procedure

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

Step 2 Click **Add New**.

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

- User ID: Enter the end user identification name. Cisco Unified Communications Manager does not permit modifying the user ID after it is created. You may use the following special characters: =, +, <, >, #,;, \,, “”, and blank spaces. **Example**: johndoe
- Password and Confirm Password: Enter five or more alphanumeric or special characters for the end user password. You may use the following special characters: =, +, <, >, #, ;, \, , “”, and blank spaces.
- Last Name: Enter the end user last name. You may use the following special characters: =, +, <, >, #, ;, \, , “”, and blank spaces. **Example**: doe
- Telephone Number: Enter the primary directory number for the end user. End users can have multiple lines on their phones. **Example**: 26640 (John Doe’s internal company telephone number)

Step 4 Click **Save**.

Add a User to an End User Group

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

Procedure

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

The Find and List Users window displays.

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

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

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

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

A list of users that matches your search criteria appears.

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

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

Step 7 Choose **Add Selected**.

Associate Phones with Users

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

Procedure

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

The Find and List Users window appears.

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

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

Step 4 Select **Device Association**.

The User Device Association window appears.

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

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

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

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

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

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

Surviveable Remote Site Telephony

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

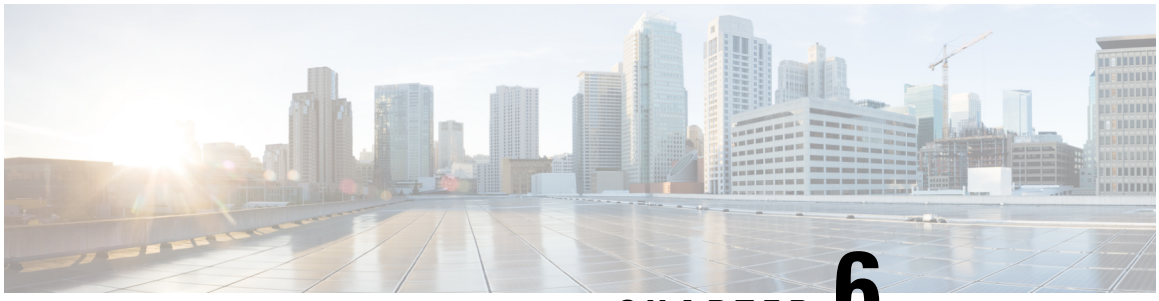
The following table describes the availability of features during failover.

Table 23: SRST feature support

Feature	Supported	Notes
New Call	Yes	
End Call	Yes	
Redial	Yes	
Answer	Yes	
Hold	Yes	
Resume	Yes	
Conference	Yes	3 way only and local mixing only.
Conference List	No	
Transfer	Yes	Consult only.
Transfer to Active Calls (Direct Transfer)	No	
Auto Answer	Yes	
Call Waiting	Yes	
Caller ID	Yes	
Unified Session Presentation	Yes	Conference is the only feature supported due to other feature limitations.
Voicemail	Yes	Voicemail will not be synchronized with other users in the Cisco Unified Communications Manager cluster.

Feature	Supported	Notes
Call Forward All	Yes	Forward state is only available on the phone that sets the forward because there are no shared line appearances in SRST mode. The Call Forward All settings are not preserved on failover to SRST from the Cisco Unified Communications Manager, or from SRST fail-back to the Communications Manager. Any original Call Forward All still active on the Communications Manager should be indicated when the device reconnects to the Communications Manager after failover.
Speed Dial	Yes	
To Voicemail (iDivert)	No	The iDivert softkey does not display.
Line Filters	Partial	Lines are supported but cannot be shared.
Park Monitoring	No	The Park softkey does not display.
Enhanced Message Waiting Indication	No	Message count badges do not appear on the phone screen. Only the Message Waiting icon displays.
Directed Call Park	No	The softkey does not display.
BLF	Partial	BLF feature key works like Speed Dial keys.
Hold Reversion	No	Calls remain on hold indefinitely.
Remote Hold	No	Calls appear as Local Hold calls.
Meet Me	No	The Meet Me softkey does not display.
PickUp	No	The softkey causes no action.
Group PickUp	No	The softkey causes no action.
Other PickUp	No	The softkey causes no action.
Malicious Call ID	No	The softkey causes no action.
QRT	No	The softkey causes no action.
Hunt Group	No	The softkey causes no action.
Intercom	No	The softkey causes no action.
Mobility	No	The softkey causes no action.
Privacy	No	The softkey causes no action.
Call Back	No	The Call Back softkey does not display.

Feature	Supported	Notes
Service URL	Yes	The programmable line key with a Service URL assigned is displayed.



CHAPTER 6

Self Care Portal Management

- Self Care Portal Overview, on page 69
- Set Up User Access to the Self Care Portal, on page 69
- Customize the Self Care Portal Display, on page 70

Self Care Portal Overview

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

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

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

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

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

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

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

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

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

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

Related Topics

Cisco Unified Communications Manager Documentation, on page xv

Set Up User Access to the Self Care Portal

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

Procedure

Step 1 In Cisco Unified Communications Manager Administration, select **User Management** > **End User**.
Step 2 Search for the user.
Step 3 Click the user ID link.
Step 4 Ensure that the user has a password and PIN configured.
Step 5 In the Permission Information section, ensure that the Groups list includes **Standard CCM End Users**.
Step 6 Select **Save**.

Customize the Self Care Portal Display

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

- Show Ring Settings
- Show Line Label Settings

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

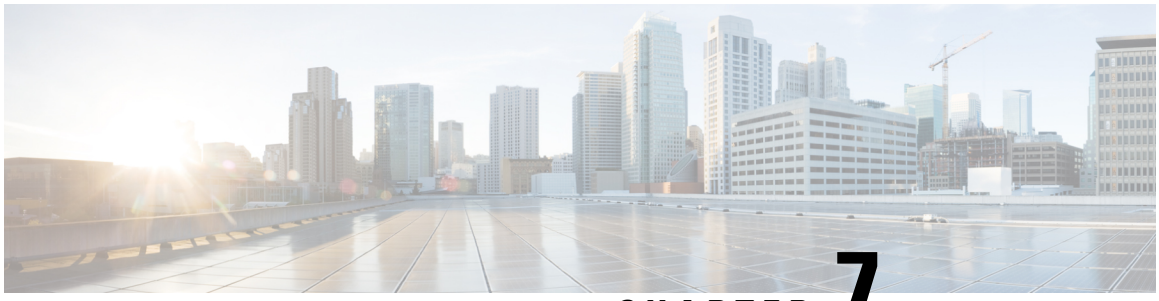
Procedure

Step 1 In Cisco Unified Communications Manager Administration, select **System** > **Enterprise Parameters**.
Step 2 In the Self Care Portal area, set the **Self Care Portal Default Server** field.
Step 3 Enable or disable the parameters that the users can access in the portal.
Step 4 Select **Save**.

PART III

Cisco IP Phone Administration

- Cisco IP Phone Security, on page 73
- Cisco IP Phone Customization, on page 85
- Phone Features and Setup , on page 89
- Corporate and Personal Directory Setup, on page 157



CHAPTER 7

Cisco IP Phone Security

- Cisco IP Phone Security Overview, on page 73
- Security Enhancements for Your Phone Network, on page 74
- View the Current Security Features on the Phone, on page 75
- View Security Profiles, on page 76
- Supported Security Features, on 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 documentation for your particular Cisco Unified Communications Manager release.

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

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

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

The Cisco IP Phone 7800 Series complies with Federal Information Processing Standard (FIPS). To function correctly, FIPS mode requires an RSA key size of 2048 bits or greater. If the RSA server certificate is not 2048 bits or greater, the phone will not register with Cisco Unified Communications Manager and `Phone failed to register. Cert key size is not FIPS compliant` displays on the phone.

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

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

Related Topics

Cisco Unified Communications Manager Documentation, on page xv
Set Up a Locally Significant Certificate, on page 78

Security Enhancements for Your Phone Network

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

The enhanced security environment includes the following features:

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

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

SIP OAuth Support

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

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

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

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

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

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

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

Where to Find More Information about Phone Security

For additional information about security, see the following:

- *Security Guide for Cisco Unified Communications Manager* (https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/security/14SU2/cucm_b_security-guide-14su2.html)
- *Cisco Unified SCCP and SIP SRST System Administration Guide* (https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cusrst/admin/sccp_sip_srst/configuration/guide/SCCP_and_SIP_SRST_Admin_Guide/srst_roadmap.html)
- *System Configuration Guide for Cisco Unified Communications Manager*, Release 14.0(1) or later (https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html).
- *Cisco IP Phone 7800 and 8800 Series Security Overview* (https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/white-paper-listing.html)

View the Current Security Features on the Phone

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

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.

Related Topics

Cisco Unified Communications Manager Documentation, on page xv

View Security Profiles

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

Procedure

Step 1 In Cisco Unified Communications Manager Administration, select **System** > **Security** > **Phone Security Profile**.

Step 2 Look at the Security Mode setting.

Related Topics

Cisco Unified Communications Manager Documentation, on page xv

Supported Security Features

The following table provides an overview of the security features that the Cisco IP Phone 7800 Series support. For more information about these features, Cisco Unified Communications Manager and Cisco IP Phone security, see the documentation for your particular Cisco Unified Communications Manager release.

Table 24: Overview of Security Features

Feature	Description
Image authentication	Signed binary files (with the extension .sbn) prevent tampering image causes a phone to fail the authentication process and rej
Customer-site certificate installation	Each Cisco IP Phone requires a unique certificate for device au for additional security, you can specify in Cisco UnifiedComm Certificate Authority Proxy Function (CAPF). Alternatively, y Configuration menu on the phone.
Device authentication	Occurs between the Cisco Unified Communications Manager s Determines whether a secure connection between the phone ar creates a secure signaling path between the entities by using T unless they can be authenticated by the Cisco Unified Commu

Feature	Description
File authentication	Validates digitally signed files that the phone downloads. T after the file creation. Files that fail authentication are not v processing.
Signaling Authentication	Uses the TLS protocol to validate that no tampering has oc
Manufacturing installed certificate	Each Cisco IP Phone contains a unique manufacturing inst permanent unique proof of identity for the phone, and allo
Secure SRST reference	After you configure a SRST reference for security and ther Administration, the TFTP server adds the SRST certificate a TLS connection to interact with the SRST-enabled router
Media encryption	Uses SRTP to ensure that the media streams between suppo the data. Includes creating a media primary key pair for the while the keys are in transport.
CAPF (Certificate Authority Proxy Function)	Implements parts of the certificate generation procedure th generation and certificate installation. The CAPF can be co behalf of the phone, or it can be configured to generate cer
Security profiles	Defines whether the phone is nonsecure or encrypted.
Encrypted configuration files	Lets you ensure the privacy of phone configuration files.
Optional disabling of the web server functionality for a phone	You can prevent access to a phone web page, which displa
Phone hardening	Additional security options, which you control from Cisco • Disable PC port • Disable PC Voice VLAN access • Disable access to web pages for a phone **Note** You can view current settings for the PC Port Disabled, GAR menu.
802.1X Authentication	The Cisco IP Phone can use 802.1X authentication to requ

Feature	Description
AES 256 Encryption	When connected to Cisco Unified Communications Manager I TLS and SIP for signaling and media encryption. This enables p that conform to SHA-2 (Secure Hash Algorithm) standards an ciphers are: • For TLS connections: • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA • For sRTP: • AEAD_AES_256_GCM • AEAD_AES_128_GCM For more information, see the Cisco Unified Communications
Elliptic Curve Digital Signature Algorithm (ECDSA) certificates	As part of Common Criteria (CC) certification, Cisco Unified C all Voice Operating System (VOS) products from version CUC

Related Topics

Cisco Unified Communications Manager Documentation, on page xv
Phone Call Security, on page 79
802.1x Authentication, on page 82
View Security Profiles, on page 76

Set Up a Locally Significant Certificate

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

Before you begin

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

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

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

Procedure

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

Step 2 From the phone, press **Applications** .

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

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

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

The phone prompts for an authentication string.

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

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

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

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

Related Topics

Cisco Unified Communications Manager Documentation, on page xv

Enable FIPS Mode

Procedure

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

Phone Call Security

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

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

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

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

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

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

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

Secure Conference Call Identification

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

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

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

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

Table 25: 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 me Security Level, call rejecte`
Secure	Meet Me	Minimum security level is nonsecure.	Secure conference bridge Conference accepts all calls.

Secure Phone Call Identification

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

A secured call is established using this process:

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

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

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

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

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

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

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

You must perform the following actions to configure 802.1X.

- Configure the other components before you enable 802.1X Authentication on the phone.
- Configure 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:

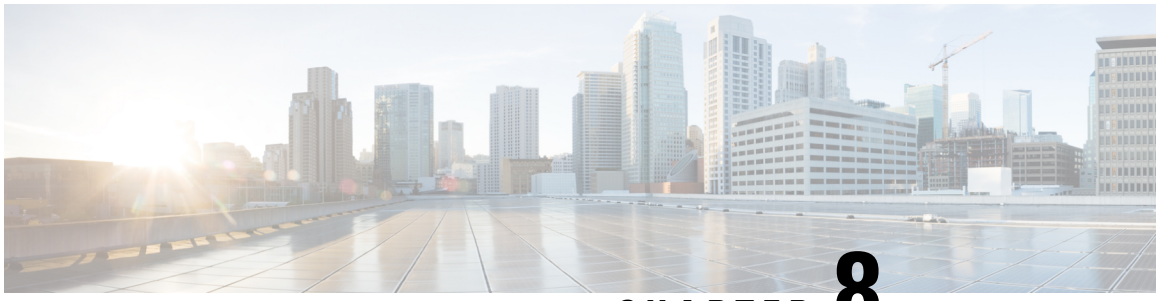
    http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

- 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.

Related Topics

Cisco Unified Communications Manager Documentation, on page xv



CHAPTER 8

Cisco IP Phone Customization

- Custom Phone Ringtones, on page 85
- Set Up Wideband Codec, on page 85
- Set Up Handset for 7811, on page 86
- Set Up Idle Display, on page 86
- Customize the Dial Tone, on page 87

Custom Phone Ringtones

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

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

For more information, see the "Custom Phone Rings and Backgrounds" chapter, Feature Configuration Guide for Cisco Unified Communications Manager.

Related Topics

Cisco Unified Communications Manager Documentation, on page xv

Set Up Wideband Codec

By default, the G.722 codec is enabled for the phone. 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

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

Step 2 Set the Advertise G.722 Codec field.

The default value of this enterprise parameter is Enabled, which means that all Cisco IP Phones that register to this Cisco Unified Communications Manager advertise G.722 to Cisco Unified Communications Manager. If each endpoint in the attempted call supports G.722 in the capabilities set, Cisco Unified Communications Manager chooses that codec for the call whenever possible.

Set Up Handset for 7811

The Cisco IP Phone 7811 ships with a narrowband or wideband handset. The administrator must configure the type of the handset for the phone to work.

Procedure

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

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

Step 3 In the Phone Configuration window set the **Wideband Handset** field:

a) For narrowband handset, set the field to **Disabled** or **Use Phone Default**.

b) For wideband handset, set the field to **Enabled**.

Step 4 Select **Save**.

Set Up Idle Display

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

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

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_tech_note09186a00801c0764.shtml

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

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

Procedure

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

Step 2 In the Idle field, enter the URL to the idle display XML Service.

Step 3 In the Idle Timer field, enter the time that the idle phone waits before displaying the idle display XML service.

Step 4 Select **Save**.

Related Topics

Cisco Unified Communications Manager Documentation, on page xv

Customize the Dial Tone

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

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

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

Procedure

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

Step 2 Select the appropriate Server.

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

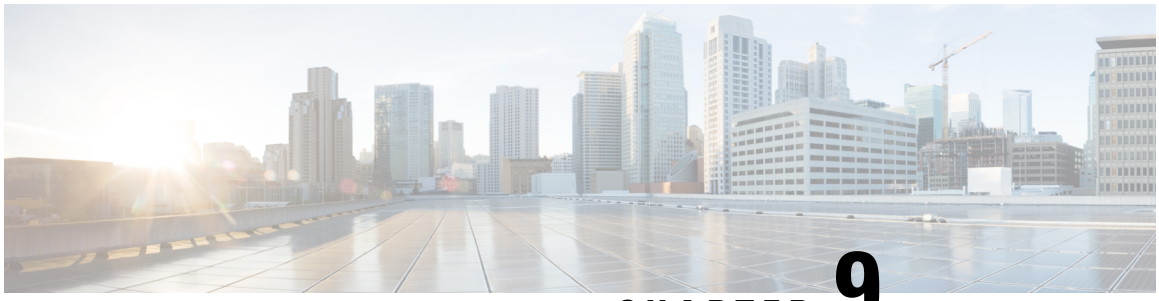
Step 4 Scroll to the Clusterwide Parameters pane.

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

- Outside
- Inside
- Default

Step 6 Select **Save**.

Step 7 Restart your phones.



CHAPTER 9

Phone Features and Setup

- Cisco IP Phone User Support, on page 89
- Telephone Features, on page 89
- Feature Buttons and Softkeys, on page 106
- Phone Feature Configuration, on page 108
- Migration of your Phone to a Multiplatform Phone Directly, on page 146
- Set Up Softkey Template, on page 146
- Phone Button Templates, on page 149
- Headset Management on Older Versions of Cisco Unified Communications Manager, on page 151

Cisco IP Phone User Support

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

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

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

Consider including the following types of information on this site:

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

Telephone Features

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 the *Cisco IP Phone 7800 Series User Guide*. See Feature Buttons and Softkeys, on page 106 for a list of features that can be configured as programmable buttons and dedicated softkeys and feature buttons.

When adding features to the phone line keys, you are limited by the number of line keys available. You cannot add more features than the number of line keys on your phone.

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 documentation for your particular Cisco Unified Communications Manager release.

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	Allows users to speed dial a phone number by entering an assigned index code (1-199) on the phone keypad. **Note** You can use Abbreviated Dialing while on-hook or off-hook. Users assign index codes from the Self Care Portal.
Actionable Incoming Call Alert	Provides different options to control the incoming call alerts. You can disable or enable the call alert. You can also activate or deactivate the caller ID display. **Note** Because the Cisco IP Phone 7811 does not have line key, it enables the call alert by default but cannot disable it. See Actionable Incoming Call Alert, Product Specific Configuration, on page 109.
AES 256 Encryption Support for Phones	Enhances security by supporting TLS 1.2 and new ciphers. For more information, see Supported Security Features, on page 76.
Agent Greeting	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. See Enable Agent Greeting, on page 132.
Any Call Pickup	Allows users to pick up a call on any line in their call pickup group, regardless of how the call was routed to the phone. See call park information in the documentation for your particular Cisco Unified Communications Manager release.

Feature	Description and More Information
Assisted Directed Call Park	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. See the call park information in the documentation for your particular Cisco Unified Communications Manager release.
Audible Message Waiting Indicator (AMWI)	A stutter tone from the handset, headset, or speakerphone indicates that a user has one or more new voice messages on a line. **Note** The stutter tone is line-specific. You hear it only when using the line with the waiting messages.
Auto Answer	Connects incoming calls automatically after a ring or two. Auto Answer works with either the speakerphone or the headset. **Note** The Cisco IP Phone 7811 does not support a headset. See directory number information in the documentation for your particular Cisco Unified Communications Manager release.
Automatic Port Synchronization	Enables the phone to synchronize the PC and SW ports to the same speed and to duplex. Only ports configured for auto negotiate change speeds. See Automatic Port Synchronization, Product Specific Configuration, on page 109.
Auto Pickup	Allows a user to use one-touch pickup functionality for call pickup features. See call pickup information in the documentation for your particular Cisco Unified Communications Manager release.
Always On Mode	Always keeps the DECT connection between the headset and base even when the user is not on a call or playing music. This feature is supported on Cisco Headset 500 Series. See Headset template management in Call Manager for more information.
Barge	Enables a user to barge into a call by establishing the three-way conference call using the built-in conference bridge of the target phone. See “cBarge” in this table.
Block External to External Transfer	Prevents users from transferring an external call to another external number. See call transfer restrictions in the documentation for your particular Cisco Unified Communications Manager release.

Feature	Description and More Information
Busy Lamp Field (BLF)	Allows a user to monitor the call state of a directory number associated with a speed-dial button on the phone. **Note** The Cisco IP Phone 7811 does not support the feature. See presence information in the documentation for your particular Cisco Unified Communications Manager release.
Busy Lamp Field (BLF) Pickup	Provides enhancements to BLF speed dial. Allows you to configure a Directory Number (DN) that a user can monitor for incoming calls. When the DN receives an incoming call, the system alerts the monitoring user, who can then pick up the call. **Note** The Cisco IP Phone 7811 does not support the feature. See call pickup information in the documentation for your particular Cisco Unified Communications Manager release..
Call Back	Provides users with an audio and visual alert on the phone when a busy or unavailable party becomes available. See call back information in the documentation for your particular Cisco Unified Communications Manager release.
Call Display Restrictions	Determines the information that will display for calling or connected lines, depending on the parties who are involved in the call. See routing and call display information in the documentation for your particular Cisco Unified Communications Manager release.
Call Forward	Allows users to redirect incoming calls to another number. Call Forward options include Call Forward All, Call Forward Busy, Call Forward No Answer, and Call Forward No Coverage. See directory number information in the documentation for your particular Cisco Unified Communications Manager release and Customize the Self Care Portal Display, on page 70.
Call Forward All Loop Breakout	Detects and prevents Call Forward All loops. When a Call Forward All loop is detected, the Call Forward All configuration is ignored and the call rings through.
Call Forward All Loop Prevention	Prevents a user from configuring a Call Forward All destination directly on the phone that creates a Call Forward All loop or that creates a Call Forward All chain with more hops than the existing Forward Maximum Hop Count service parameter allows.
Call Forward Configurable Display	Allows specifying information that appears on a phone when a call is forwarded. This information can include the caller name, caller number, redirected number, and original dialed number. See directory number information in the documentation for your particular Cisco Unified Communications Manager release.

Feature	Description and More Information
Call Forward Destination Override	Allows you to override Call Forward All (CFA) in cases where the CFA target places a call to the CFA initiator. This feature allows the CFA target to reach the CFA initiator for important calls. The override works whether the CFA target phone number is internal or external. See directory number information in the documentation for your particular Cisco Unified Communications Manager release.
Call Forward Notification	Allows you to configure the information that the user sees when receiving a forwarded call. See Set Up Call Forward Notification, on page 134.
Call History for Shared Line	Allows you to view shared line activity in the phone Call History. This feature will: • Log missed calls for a shared line • Log all answered and placed calls for a shared line See Call History Shared Line, Product Specific Configuration, on page 109.
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.
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.
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. **Note** 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.
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 directory number information in the documentation for your particular Cisco Unified Communications Manager release.
Call Waiting Ring	Provides Call Waiting users with the option of an audible ring instead of the standard beep. Options are Ring, Ring Once, Flash Only, and Beep Only. See directory number information in the documentation for your particular Cisco Unified Communications Manager release.

Feature	Description and More Information
Caller ID	Caller identification such as a phone number, name, or other descriptive text appear on the phone display. See routing, call display, and directory number information in the documentation for your particular Cisco Unified Communications Manager release.
Caller ID Blocking	Allows a user to block their phone number or name from phones that have caller identification enabled. See routing and directory number information in the documentation for your particular Cisco Unified Communications Manager release.
Calling Party Normalization	Calling party normalization presents phone calls to the user with a dialable phone number. Any escape codes are added to the number so that the user can easily connect to the caller again. The dialable number is saved in the call history and can be saved in the Personal Address Book.
CAST for SIP	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. The main software supported is Cisco Jabber.
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, refer to the "Barge" chapter, Feature Configuration Guide for Cisco Unified Communications Manager.
Cisco Extension Mobility	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. 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.
Cisco Extension Mobility Cross Cluster (EMCC)	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. **Note** Configure Cisco Extension Mobility on Cisco IP Phones before you configure EMCC.
Cisco IP Phone 7811 Support	Provides support for the Cisco IP Phone 7811. The phone does not support headset, display backlight, intercom, AUX Port, programmable feature button, and line keys.
Cisco Sans 2.0 Latin Font Support	Introduces the Cisco Sans 2.0 font for all Latin characters in the Call Display.

Feature	Description and More Information
Cisco Unified Communications Manager Express (Unified CME) Version Negotiation	The Cisco Unified Communication Manager Express uses a special tag in the information sent to the phone to identify itself. This tag enables the phone to provide services to the user that the switch supports. See: • *Cisco Unified Communications Manager Express System Administrator Guide* • *Cisco Unified Communications Manager Express Interaction*.
Cisco Unified Video Advantage (CUVA)	Allows users to make video calls by using a Cisco IP Phone, a personal computer, and an external video camera. **Note** Configure the Video Capabilities parameter in the Product Specific Configuration Layout section in Phone Configuration. See the Cisco Unified Video Advantage documentation.
Cisco WebDialer	Allows users to make calls from web and desktop applications.
Classic Ringtone	Supports narrowband and wideband ringtones. The feature makes the available ringtones common with other Cisco IP Phones. See Custom Phone Ringtones, on page 85.
Conference	Allows a user to talk simultaneously with multiple parties by calling each participant individually. Conference features include Conference and Meet Me. Allows a noninitiator in a standard (adhoc) conference to add or remove participants; also allows any conference participant to join together two standard conferences on the same line. The Advance Adhoc Conference service parameter, disabled by default in Cisco Unified Communications Manager Administration, allows you to enable these features. **Note** Be sure to inform your users whether these features are activated.
Confidential Access Level (CAL)	Controls whether a call can be completed based on the CAL configuration in the Cisco Unified Communications Manager. When CAL is enabled, the user sees information about the call in a CAL message. The phone displays the CAL message for the duration of the call. If a call fails due to an incompatible CAL, the phone displays a failure message. You set up the failure message that the user sees.
Configurable Energy Efficient Ethernet (EEE) for Port and Switch	Provides a method to control EEE functions on personal computer port and switch port by enabling or disabling EEE. The feature controls both type of ports individually. The default value is Enabled. See Energy Efficient Ethernet for Port and Switch, Product Specific Configuration, on page 109.

Feature	Description and More Information
Configurable RTP/sRTP Port Range	Provides a configurable port range (2048 to 65535) for Real-Time Transport Protocol (RTP) and secure Real-Time Transport Protocol (sRTP). The default RTP and sRTP port range is 16384 to 32764. You configure the RTP and sRTP port range in the SIP Profile. See Set Up RTP/sRTP Port Range, on page 138.
CTI Applications	A computer telephony integration (CTI) route point can designate a virtual device to receive multiple, simultaneous calls for application-controlled redirection.
Device Invoked Recording	Provides end users with the ability to record their telephone calls via a softkey. In addition administrators may continue to record telephone calls via the CTI User Interface. See Device Invoked Recording, Product Specific Configuration, on page 109.
Directed Call Park	Allows a user to transfer an active call to an available directed call park number that the user dials or speed dials. A Call Park BLF button indicates whether a directed call park number is occupied and provides speed-dial access to the directed call park number. **Note** If you implement Directed Call Park, avoid configuring the Park softkey. This prevents users from confusing the two Call Park features. See call park information in the documentation for your particular Cisco Unified Communications Manager release.
Disable Line Key Barge	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: • Default: Press Line Key can conference into the call. • Off: Press Line Key Barge a new call. • Turn on softkey: Press Line Key turns on softkeys configured in remote-in-use and user can conference into the call through cBarge. **Note** The Cisco IP Phone 7811 does not support the feature.
Distinctive Ring	Allows users to hear different ring types depending on whether the call was originated from an internal station or external call coming from a trunk. Internal calls generate one ring, while external calls generate two rings with a very short pause between the rings. No configuration is required. See call pickup information in the documentation for your particular Cisco Unified Communications Manager release.
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.

Feature	Description and More Information
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. When enabled, the user sees the DND icon on their phone screen. If multilevel precedence and preemption (MLPP) is configured and the user receives a precedence call, the phone will ring with a special ringtone. See Set Up Do Not Disturb, on page 132.
EnergyWise	Enables an IP Phone to sleep (power down) and wake (power up) at predetermined times, to promote energy savings. **Note** The Cisco IP Phone 7811 does not support this feature. See Power Save Plus (EnergyWise), Product Specific Configuration, on page 109 .
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).
Extension Mobility Size Safe and Feature Safe	With Feature Safe, your phone can use any phone button template that has the same number of line buttons that the phone model supports. Size Safe allows your phone to use any phone button template that is configured on the system.
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.
Headset Sidetone Control	Allows an administrator to set the sidetone level of a wired headset. **Note** The Cisco IP Phone 7811 does not support a headset.
Group Call Pickup	Allows a user to answer a call that is ringing on a directory number in another group. See call pickup information in the documentation for your particular Cisco Unified Communications Manager release.
Hold Reversion	Limits the amount of time that a call can be on hold before reverting back to the phone that put the call on hold and alerting the user. 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. 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.
Hold Status	Enables phones with a shared line to distinguish between the local and remote lines that placed a call on hold.

Feature	Description and More Information
Hold/Resume	Allows the user to move a connected call from an active state to a held state. • No configuration required unless you want to use Music On Hold. See "Music On Hold" in this table for information. • See "Hold Reversion" in this table.
HTTP Download	Enhances the file download process to the phone to use HTTP by default. If the HTTP download fails, the phone reverts to using the TFTP download.
HTTPS for Phone Services	Increases security by requiring communication using HTTPS. **Note** IP Phones can be HTTPS clients; they cannot be HTTPS servers. See HTTPS for Phone Services, Product Specific Configuration, on page 109.
Hunt Group	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. You can have either the hunt group name or the pilot number display on the Incoming Call Alert. See hunt groups and routing plans in the documentation for your particular Cisco Unified Communications Manager release.
Improve Caller Name and Number Display	Improves the display of caller names and numbers. If the Caller Name is known then the Caller Number is displayed instead of unknown.
Incoming Call Toast Timer	Allows you to set the length of time that an incoming call toast (notification) appears on the phone screen. See Incoming Call Toast Timer, Product Specific Configuration, on page 109 .
Intercom	Allows users to place and receive intercom calls using programmable phone buttons. You can configure intercom line buttons to: • Directly dial a specific intercom extension. • Initiate an intercom call and then prompt the user to enter a valid intercom number. **Note** If your user logs into the same phone on a daily basis 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. The Cisco IP Phone 7811 does not support this feature.

Feature	Description and More Information
IPv6-only Support	IPv6-only support is provided in standalone or in configuration with IPv4-only. See Configure Network Settings, on page 45. For more details about IPv6 deployment, see the IPv6 Deployment Guide for Cisco Collaboration Systems Release 12.0.
Jitter Buffer	The Jitter Buffer feature handles jitter from 10 milliseconds (ms) to 1000 ms for both audio and video streams.
Join	Allows users to combine two calls that are on one line to create a conference call and remain on thecall. **Note** Because Cisco IP Phone 7811 has only one line, the phone uses the Calls softkey to join two calls in the same line. See Join and Direct Transfer Policy, Product Specific Configuration, on page 109 .
Join Across Lines	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. **Note** Because Cisco IP Phone 7811 has only one line, it does not support this feature. See Join and Direct Transfer Policy, Product Specific Configuration, on page 109 .
Line Display Enhancement	Improves the call display by removing the central dividing line when it is not required. This feature applies to the Cisco IP Phone 7841 only.
Line Status for Call Lists	Allows the user to see the Line Status availability status of monitored line numbers in the Call History list. The Line Status states are • Unknown • Idle • Busy • DND See Enable BLF for Call Lists, on page 135.
Line Text Label	Sets a text label for a phone line instead of the directory number. See Set the Label for a Line, on page 145.
Log out of hunt groups	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. See hunt group information in the documentation for your particular Cisco Unified Communications Manager release and Set Up Softkey Template, on page 146.

Feature	Description and More Information
Malicious Caller Identification (MCID)	Allows users to notify the system administrator about suspicious calls that are received.
Meet Me Conference	Allows a user to host a Meet Me conference in which other participants call a predetermined number at a scheduled time.
Message Waiting	Defines directory numbers for message waiting on and off indicators. A directly-connected voice-message system uses the specified directory number to set or to clear a message waiting indication for a particular Cisco IP Phone. See message waiting and voicemail information in the documentation for your particular Cisco Unified Communications Manager release.
Message Waiting Indicator	A light on the handset that indicates that a user has one or more new voice messages. See message waiting and voicemail information in the documentation for your particular Cisco Unified Communications Manager release.
Minimum Ring Volume	Sets a minimum ringer volume level for an IP phone. See Minimum Ring Volume, Product Specific Configuration, on page 109 .
Missed Call Logging	Allows a user to specify whether missed calls will be logged in the missed calls directory for a given line appearance. See directory information in the documentation for your particular Cisco Unified Communications Manager release.
Mobile Connect	Enables users to manage business calls using a single phone number and pick up in-progress calls on the desk phone and a remote device such as a mobile phone. Users can restrict the group of callers according to phone number and time of day.
Mobile and Remote Access Through Expressway	Allows remote workers to easily and securely connect into the corporate network without using a virtual private network (VPN) client tunnel. See Mobile and Remote Access Through Expressway, on page 139.
Mobile Voice Access	Extends Mobile Connect capabilities by allowing users to access an interactive voice response (IVR) system to originate a call from a remote device such as a cellular phone.
Monitoring and Recording	Allows a supervisor to silently monitor an active call. The supervisor cannot be heard by either party on the call. The user might hear a monitoring audible alert tone during a call when it is being monitored. 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. **Note** When an active call is being monitored or recorded, the use can receive or place intercom calls; however, if the user place an intercom call, the active call will be put on hold, which causes the recording session to terminate and the monitoring session to suspend. To resume the monitoring session, the party whose call is being monitored must resume the call. See Set Up Monitoring and Recording, on page 133.

Feature	Description and More Information
Multilevel Precedence and Preemption	Enables the user to make and receive urgent or critical calls in some specialized environments, such as military or government offices. See Multilevel Precedence and Preemption, on page 146.
Multiple Calls Per Line Appearance	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. 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. See directory number information in the documentation for your particular Cisco Unified Communications Manager release.
Music On Hold	Plays music while callers are on hold.
Mute	Mutes the handset or headset microphone.
New Phone Hardware	Provides updated hardware versions of the Cisco IP Phone 7821, 7841, and 7861. The new phones do not support firmware releases prior to 10.3(1).
No Alert Name	Makes it easier for end users to identify transferred calls by displaying the original caller's phone number. The call appears as an Alert Call followed by the caller's telephone number.
Onhook Dialing	Allows a user to dial a number without going off hook. The user can then either pick up the handset or press Dial.
Other Group Pickup	Allows a user to answer a call ringing on a phone in another group that is associated with the user's group. See call pickup information in the documentation for your particular Cisco Unified Communications Manager release.
Outbound Roll Over	Allows users to make a call when the number of calls for a line exceeds the maximum number of calls (MNC). This feature is configured on Cisco Unified Communication Manager by navigating **Device > Phone**. It is disabled by default. **Note** The Cisco IP Phone 7811 does not support this feature.
Pause in Speed Dial	Users can set up the speed-dial feature to reach destinations that require Forced Authorization Code (FAC) or Client Matter Code (CMC), dialing pauses, and additional digits (such as a user extension, a meeting access code, or a voicemail password) without manual intervention. When the user presses the speed dial, the phone establishes the call to the specified DN and sends the specified FAC, CMC, and DTMF digits to the destination and inserts the necessary dialing pauses.

Feature	Description and More Information
Peer Firmware Sharing	Provides the following advantages in high-speed campus LAN settings: • Limits congestion on TFTP transfers to centralized remote TFTP servers • Eliminates the need to manually control firmware upgrades • Reduces phone downtime during upgrades when large numbers of devices are reset simultaneously Peer Firmware Sharing may also aid in firmware upgrades in branch/remote office deployment scenarios that run over bandwidth-limited WAN links. See Peer Firmware Sharing, Product Specific Configuration, on page 109 .
Phone Display Message for Extension Mobility Users	This feature enhances the phone interface for the Extension Mobility user by providing friendly messages.
PLK Support for Queue Statistics	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. **Note** The Cisco IP Phone 7811 does not support this feature. See Set Up Softkey Template, on page 146.
Plus Dialing	Allows the user to dial E.164 numbers prefixed with a plus (+) sign. 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.
Privacy	Prevents users who share a line from adding themselves to a call and from viewing information on their phone display about the call of the other user. **Note** The Cisco IP Phone 7811 does not support privacy. See barge information in the documentation for your particular Cisco Unified Communications Manager release.
Private Line Automated Ringdown (PLAR)	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. The administrator can configure a delay of up to 15-seconds. This allows the user time to place a call before the phone defaults to the hotline number. The timer is configurable through the parameter **Off Hook To First Digit Timer** under **Device** > **Device Settings** > **SIP Profile**. For more information, refer to *Feature Configuration Guide for Cisco Unified Communications Manager*. See directory number information in the documentation for your particular Cisco Unified Communications Manager release.
Problem Report Tool (PRT)	Submit phone logs or report problems to an administrator. See Problem Report Tool, on page 143.

Feature	Description and More Information
Programmable Feature Buttons	You can assign features, such as New Call, Call Back, and Forward All to line buttons. **Note** The Cisco IP Phone 7811 does not support this feature. See phone button templates in the documentation for your particular Cisco Unified Communications Manager release.
Quality Reporting Tool (QRT)	Allows users to submit information about problem phone calls by pressing a button. QRT can be configured for either of two user modes, depending upon the amount of user interaction desired with QRT.
Recents	Allows you to enable/disable the Recents softkey on a phone.
Redial	Allows users to call the most recently dialed phone number by pressing a button or the Redial softkey.
Reroute Direct Calls to Remote Destination to Enterprise Number	Reroutes a direct call to a user's mobile phone to the enterprise number (desk phone). For an incoming call to remote destination (mobile phone), only remote destination rings; desk phone does not ring. When the call is answered on their mobile phone, the desk phone displays a Remote In Use message. During these calls, users can make use of various features of their mobile phone. See Cisco Unified Mobility information in the documentation for your particular Cisco Unified Communications Manager release.
Remote Port Configuration	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. **Note** If the ports are configured for Remote Port Configuration in Cisco Unified Communications Manager, the data cannot be changed on the phone. See Remote Port Configuration, Product Specific Configuration, on page 109 .
Ringtone Setting	Identifies ring type used for a line when a phone has another active call. See directory number information in the documentation for your particular Cisco Unified Communications Manager release and Custom Phone Ringtones, on page 85.
RTCP Hold For SIP	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.

Feature	Description and More Information
Secure Conference	Allows secure phones to place conference calls using a secured conference bridge. As new participants are added by using Confrn, Join, cBarge softkeys or MeetMe conferencing, the secure call icon displays as long as all participants use secure phones. The Conference List displays the security level of each conference participant. Initiators can remove nonsecure participants from the Conference List. Noninitiators can add or remove conference participants if the Advanced Adhoc Conference Enabled parameter is set. See conference information in the documentation for your particular Cisco Unified Communications Manager release and Supported Security Features, on page 76
Secure EMCC	Improves the EMCC feature by providing enhanced security for a user logging into their phone from a remote office.
Services	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.
Services URL button	Allows users to access services from a programmable button rather than by using the Services menu on a phone. **Note** The Cisco IP Phone 7811 does not support this feature.
Serviceability for SIP Endpoints	Enables administrators to quickly and easily gather debug information from phones. This feature uses SSH to remotely access each IP phone. SSH must be enabled on each phone for this feature to function.
Shared Line	Allows a user with multiple phones to share the same phone number or allows a user to share a phone number with a coworker. See directory number information in the documentation for your particular Cisco Unified Communications Manager release.
Show Calling ID and Calling Number	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. 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. See “Caller ID” in this table.
Show Duration for Call History	Displays the time duration of placed and received calls in the Call History details. If the duration is greater than or equal to one hour, the time is displayed in the Hour, Minute, Second (HH:MM:SS) format. If the duration is less than one hour, the time is displayed in the Minute, Second (MM:SS) format. If the duration is less than one minute, the time is displayed in the Second (SS) format.

Feature	Description and More Information
Simplify Extension Mobility Login with Cisco Headsets	Enables users to sign into Extension Mobility with their Cisco headsets. When the phone is in Mobile and Remote Access through Expressway (MRA) mode, the user can use the headset to sign into the phone Headset login with MRA requires Cisco Unified Communications Manager(UCM) Release 11.5(1)SU8,11.5(1)SU.9, 12.5(1)SU3 or later.
Speed Dial	Dials a specified number that has been previously stored.
SSH Access	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. See SSH Access, Product Specific Configuration, on page 109 .
Time-of-Day Routing	Restricts access to specified telephony features by time period. See time and date information in the documentation for your particular Cisco Unified Communications Manager release.
Time Zone Update	Updates the Cisco IP Phone with time zone changes. See time and date information in the documentation for your particular Cisco Unified Communications Manager release..
Transfer	Allows users to redirect connected calls from their phones to another number. Some JTAPI/TAPI applications are not compatible with the Join and Direct Transfer feature implementation on the 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. See Join and Direct Transfer Policy, Product Specific Configuration, on page 109 .
TVS	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. The Security Setting menu on the phone displays the TVS information.
UCR 2008	The Cisco IP Phones support Unified Capabilities Requirements (UCR) 2008 by providing the following functions: • Support for Federal Information Processing Standard(FIPS) • Support for 80-bit SRTCP Tagging As an IP Phone administrator, you must set up specific parameters in Cisco Unified Communications Manager Administration. See UCR 2008 Setup, on page 136.
Voice Message System	Enables callers to leave messages if calls are unanswered.

Feature	Description and More Information
Web Access Disabled by Default	Enhances security by disabling access to all web services, such as HTTP. Users can only access web services if you enable web access. See UCR 2008 Setup, on page 136.
Whisper Announcement	Plays a brief, prerecorded message to an agent just before the agent connects with each caller. The announcement plays only to the agent; the caller hears ringing (based on existing ring tone patterns) while the announcement plays. The content of the announcement can contain information about the caller that helps prepare the agent to handle the call. The information can include caller language preference, choices the caller made from a menu (Sales, Service), customer status (Platinum, Gold, Regular), and so on.
Whisper Coaching	An enhancement to silent call monitoring feature that allows supervisors to talk to agents during a monitoring session. This feature provides applications the ability to change the current monitoring mode of a monitoring call from Silent Monitoring to Whisper Coaching and vice versa.

Related Topics

Cisco Unified Communications Manager Documentation, on page xv

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. A “Supported” entry 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.

Note The Cisco IP Phone 7811 does not have programmable feature buttons.

For information about configuring programmable feature buttons, see Phone Button Templates, on page 149.

Table 26: Features with Corresponding Buttons and Softkeys

Feature Name	Dedicated Feature Button	Programmable Feature Button	Softkey
Answer		Supported	Supported
Barge			Supported
Call Back		Supported	Supported
Call Forward All		Supported	Supported
Call Park		Supported	Supported

Feature Name	Dedicated Feature Button	Programmable Feature Button	Softkey
Call Park Line Status		Supported	
Call Pickup (Pick Up)		Supported	Supported
Call Pickup Line Status		Supported	
Conference	Supported		Supported (only displayed during connected call conference scenario)
Divert			Supported
Do Not Disturb		Supported	Supported
Executive - Access to **Settings** > **Assistant** menu		Supported	
Executive Assistant - Access to **Settings** > **Executive** menu		Supported	
Group Pickup (Group Pick Up)		Supported	Supported
Hold	Supported		Supported
Hunt Groups		Supported	Supported
Intercom		Supported	
Malicious Call Identification (MCID)		Supported	Supported
Meet Me		Not Supported	Not Supported
Mobile Connect (Mobility)		Supported	Supported
Mute	Supported		
Other Pickup		Supported	Supported
Privacy		Supported	
Queue Status		Supported	
Quality Reporting Tool (QRT)		Supported	Supported
Record	Not supported	Not supported	Supported
Redial		Supported	Supported
Speed Dial		Supported	Supported
Speed Dial Line Status		Supported	

Feature Name	Dedicated Feature Button	Programmable Feature Button	Softkey
Transfer	Supported		Supported (only displayed during connected call transfer scenario)

Phone Feature Configuration

You can set up phones to have a variety of features, based on the needs of your users. You can apply features to all phones, a group of phones, or to individual phones.

When you set up features, the Cisco Unified Communications Manager Administration window displays information that is applicable to all phones and information that is applicable to the phone model. The information that is specific to the phone model is in the Product Specific Configuration Layout area of the window.

For information on the fields applicable to all phone models, see the Cisco Unified Communications Manager documentation.

When you set a field, the window that you set the field in is important because there is a precedence to the windows. The precedence order is:

1. Individual phones (highest precedence)
2. Group of phones
3. All phones (lowest precedence)

For example, if you don't want a specific set of users to access the phone Web pages, but the rest of your users can access the pages, you:

1. Enable access to the phone web pages for all users.
2. Disable access to the phone web pages for each individual user, or set up a user group and disable access to the phone web pages for the group of users.
3. If a specific user in the user group did need access to the phone web pages, you could enable it for that particular user.

Set Up Phone Features for All Phones

Procedure

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

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

Step 3 Set the fields you want to change.

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

Step 5 Click **Save**.
Step 6 Click **Apply Config**.
Step 7 Restart the phones.

Note
This will impact all phones in your organization.

Set Up Phone Features for a Group of Phones

Procedure

Step 1 Sign in to Cisco Unified Communications Manager Administration as an administrator.
Step 2 Select **Device** > **Device Settings** > **Common Phone Profile**.
Step 3 Locate the profile.
Step 4 Navigate to the Product Specific Configuration Layout pane and set the fields.
Step 5 Check the **Override Enterprise Settings** check box for any changed fields.
Step 6 Click **Save**.
Step 7 Click **Apply Config**.
Step 8 Restart the phones.

Set Up Phone Features for a Single Phone

Procedure

Step 1 Sign in to Cisco Unified Communications Manager Administration as an administrator.
Step 2 Select **Device** > **Phone**
Step 3 Locate the phone associated with the user.
Step 4 Navigate to the Product Specific Configuration Layout pane and set the fields.
Step 5 Check the **Override Common Settings** check box for any changed fields.
Step 6 Click **Save**.
Step 7 Click **Apply Config**.
Step 8 Restart the phone.

Product Specific Configuration

The following table describes the fields in the Product Specific Configuration Layout pane.

Table 27: Product Specific Configuration Fields

Field Name	Field Type or Choices	Default	Description and Usage Guidelines
Disable Speakerphone	Checkbox	Unchecked	Turns off the speakerphone capability of the phone.
Disable Speakerphone and Headset	Checkbox	Unchecked	Turns off the speakerphone and headset capability of the phone.
Disable Handset	Checkbox	Unchecked	Turns off the handset capability of the phone.
PC Port	Disabled Enabled	Enabled	Controls the ability to use the PC port to connect a computer into the LAN.
Settings Access	Disabled Enabled Restricted	Enabled	Enables, disables, or restricts access to local phone configuration settings in the Settings app. • Disabled—The Settings menu does not display any options. • Enabled—All entries in the Settings menu are accessible. • Restricted—Only the Phone settings menu is accessible.
Gratuitous ARP	Disabled Enabled	Disabled	Enables or disables the ability for the phone to learn MAC addresses from Gratuitous ARP. This capability is required to monitor or record voice streams.
PC Voice VLAN Access	Disabled Enabled	Enabled	Indicates whether the phone will allow a device attached to the PC (access) port to access the Voice VLAN. • Disabled—The computer can't send and receive data on the Voice VLAN or from the phone. • Enabled—The computer can send and receive data from the Voice VLAN or from the phone. Set this field to Enabled if an application is being run on the computer that to monitor phone traffic. These applications could include monitoring and recording applications, and the use of network monitoring software for analysis purposes.
Video Capabilities	Disabled Enabled	Disabled	Allows users to make video calls by using a Cisco IP Phone, a personal computer, and a video camera.
Web Access	Disabled Enabled	Disabled	Enables or disables access to the phone web pages through a web browser. **Caution** If you enable this field, you may expose sensitive information about the phone.

Field Name	Field Type or Choices	Default	Description and Usage Guidelines
Disable TLS 1.0 and TLS 1.1 for Web Access	Disabled Enabled	Enabled	Controls the use of TLS 1.2 for a web server connection. • Disabled—A phone configured for TLS1.0, TLS 1.1, or TLS1.2 can function as a HTTPs server. • Enabled—Only a phone configured for TLS1.2 can function as a HTTPs server.
TLS Client Min Version	TLS 1.0 TLS 1.1 TLS 1.2	TLS 1.2	Specifies the minimum TLS version required by the phone to establish a TLS connection. This parameter is available when the phone acts as a client. If the TLS version on the server side is older than the required minimum TLS version on the phone, the TLS connection will be rejected. • **TLS 1.0**: The TLS client (phone) supports the versions of TLS from 1.0 to 1.2. • **TLS 1.1**: The TLS client (phone) supports TLS 1.1 and TLS 1.2. If the TLS version in server is lower than 1.1, for example, 1.0, then the connection can't be established. • **TLS 1.2**: The TLS client (phone) supports TLS 1.2 only. If the TLS version in server is lower than 1.2, for example, 1.0 or 1.1, then the connection can't be established. **Note** This parameter is unavailable for the wireless networks.
Enbloc Dialing	Disabled Enabled	Disabled	Controls the dialing method. • Disabled—The Cisco Unified Communications Manager waits for the interdigit timer to expire when there is a dial plan or route pattern overlap. • Enabled—The entire dialed string is sent to Cisco Unified Communications Manager once the dialing is complete. To avoid the T.302 timer timeout, we recommend that you enable Enbloc Dialing whenever there is a dialplan or route pattern overlap. Forced Authorization Codes (FAC) or Client Matter Codes (CMC) do not support the Enbloc Dialing. If you use FAC or CMC to manage call access and accounting, then you cannot use this feature.

Field Name	Field Type or Choices	Default	Description and Usage Guidelines
Days Backlight Not Active	Days of the week		Defines the days that the backlight does not turn on automatically at the time specified in the Backlight On Time field. Choose the day or days from the drop-down list. To choose more than one day, **Ctrl+click** each day that you want.
Backlight On Time	hh:mm		Defines the time each day that the backlight turns on automatically (except on the days specified in the Backlight Display Not Active field). Enter the time in this field in 24 hour format, where 0:00 is midnight. For example, to automatically turn the backlight on at 07:00 a.m. (0700), enter 07:00. To turn the backlight on at 02:00 p.m. (1400), enter 14:00. If this field is blank, the backlight automatically turns on at 0:00.
Backlight On Duration	hh:mm		Defines the length of time that the backlight remains on after turning on at the time specified in the Backlight On Time field. For example, to keep the backlight on for 4 hours and 30 minutes after it turns on automatically, enter 04:30. If this field is blank, the phone turns off at the end of the day (0:00). If Backlight On Time is 0:00 and the backlight on duration is blank (or 24:00), the backlight does not turn off.
Backlight Idle Timeout	hh:mm		Defines the length of time that the phone is idle before the backlight turns off. Applies only when the backlight was off as scheduled and was turned on by a user (by pressing a button on the phone or lifting the handset). For example, to turn the backlight off when the phone is idle for 1 hour and 30 minutes after a user turns the backlight on, enter 01:30.
Backlight On When Incoming Call	Disabled Enabled	Enabled	Turns the backlight on when there is an incoming call.

Field Name	Field Type or Choices	Default	Description and Usage Guidelines
Enable Power Save Plus	Days of the week		Defines the schedule of days for which the phone powers off. Choose the day or days from the drop-down list. To choose more than one day, **Ctrl+click** each day that you want. When Enable Power Save Plus is turned on, you receive a message that warns about emergency (e911) concerns. **Caution** While Power Save Plus Mode (the "Mode") is in effect, endpoints that are configured for the mode are disabled for emergency calling and from receiving inbound calls. By selecting this mode, you agree to the following: (i) You take full responsibility for providing alternate methods for emergency calling and receiving calls while the mode is in effect; (ii) Cisco has no liability in connection with your selection of the mode and all liability in connection with enabling the mode is your responsibility; and (iii) You fully inform users of the effects of the mode on calls, calling and otherwise. To disable Power Save Plus, you must uncheck the Allow EnergyWise Overrides check box. If the Allow EnergyWise Overrides remains checked but no days are selected in the Enable Power Save Plus field, Power Save Plus is not disabled.
Phone On Time	hh:mm		Determines when the phone automatically turns on for the days that are in the Enable Power Save Plus field. Enter the time in this field in 24-hour format, where 00:00 is midnight. For example, to automatically power up the phone at 07:00 a.m. (0700), enter 07:00. To power up the phone at 02:00 p.m. (1400), enter 14:00. The default value is blank, which means 00:00. The Phone On Time must be at least 20 minutes later than the Phone Off Time. For example, if the Phone Off Time is 07:00, the Phone On Time must be no earlier than 07:20.

Field Name	Field Type or Choices	Default	Description and Usage Guidelines
Phone Off Time	hh:mm		Defines the time of day that the phone powers down for the days that are selected in the Enable Power Save Plus field. If the Phone On Time and the Phone Off Time fields contain the same value, the phone does not power down. Enter the time in this field in 24-hour format, where 00:00 is midnight. For example, to automatically power down the phone at 7:00 a.m. (0700), enter 7:00. To power down the phone at 2:00 p.m. (1400), enter 14:00. The default value is blank, which means 00:00. The Phone On Time must be at least 20 minutes later than the Phone Off Time. For example, if the Phone Off Time is 7:00, the Phone On Time must be no earlier than 7:20. For more information, see Set Up Idle Display, on page 86.
Phone Off Idle Timeout	hh:mm		Indicates the length of time that the phone must be idle before the phone powers down. The timeout occurs under the following conditions: • When the phone was in Power Save Plus mode, as scheduled, and was taken out of Power Save Plus mode because the phone user pressed the Select key. • When the phone is repowered by the attached switch. • When the Phone Off Time is reached but the phone is in use.
Enable Audible Alert	Checkbox	Unchecked	When enabled, instructs the phone to play an audible alert starting 10 minutes before the time that the Phone Off Time field specifies. This check box applies only if the Enable Power Save Plus list box has one or more days selected.
EnergyWise Domain	Up to 127 characters		Identifies the EnergyWise domain that the phone is in.
EnergyWise Secret	Up to 127 characters		Identifies the security secret password that is used to communicate with the endpoints in the EnergyWise domain.

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

Field Name	Field Type or Choices	Default	Description and Usage Guidelines
Logging Display	Disabled Enabled PC Controlled	Disabled	Selects what type of console logging is allowed. This option does not control the generation of logs—just whether the logs display. • Disabled—Indicates that logging doesn't display to the console, nor to the connected downstream port. • Enabled—Indicates that logs are always sent to the console and to the downstream port. Use Enabled to force logs on, so they can be captured with a packet sniffer. • PC Controlled—Indicates that the workstation attached to the PC port controls whether logging is enabled.
Recording Tone	Disabled Enabled	Disabled	Controls the playing of the tone when a user is recording a call.
Recording Tone Local Volume	Integer 0–100	100	Controls the volume of the recording tone to the local user.
Recording Tone Remote Volume	Integer 0–100	50	Controls the volume of the recording tone to the remote user.
Recording Tone Duration	Integer 1–3000 milliseconds		Controls the duration of the recording tone.
"more" Soft Key Timer	Integer 0, 5–30 seconds	5	Controls the duration that a row of secondary softkeys is displayed before the phone displays the initial set of softkeys. 0 disables the timer.
Log Server	String of up to 256 characters		Identifies the IPv4 syslog server for phone debug output. The format for the address is: `address:<port>@@base=<0-7>;pfs=<0-1>`
Remote Log	Disabled Enabled	Disabled	Controls the ability to send logs to the syslog server.

Field Name	Field Type or Choices	Default	Description and Usage Guidelines
Log Profile	Default Preset Telephony SIP UI Network Media Upgrade Accessory Security Wi-Fi VPN Energywise MobileRemoteAc	Preset	Specifies the predefined logging profile. • Default—Default debug logging level • Preset—Does not overwrite the phone local debug logging setting • Telephony—Logs information about Telephony or call features • SIP—Logs information about SIP signaling • UI—Logs information about the phone user interface • Network—Logs network information • Media—Logs media information • Upgrade—Logs upgrade information • Accessory—Logs accessory information • Security—Logs security information • Wi-Fi—Logs Wi-Fi information • VPN—Logs virtual private network information • Energywise—Logs energy-savings information • MobileRemoteAC—Logs Mobile and Remote Access through Expressway information
IPv6 Log Server	String of up to 256 characters		Identifies the IPv6 syslog server for phone debug output. The format for the address is: `[address]:<port>@@base=<0-7>;pfs=<0-1>`
Outbound Rollover	Disabled Enabled	Disabled	Allows users to make a call when the number of calls for a line exceeds the maximum number of calls (MNC). The Cisco IP Phone 7811 does not support this field.
Cisco Discovery Protocol (CDP): Switch Port	Disabled Enabled	Enabled	Controls Cisco Discovery Protocol on the SW port of the phone.
Cisco Discovery Protocol (CDP): PC Port	Disabled Enabled	Enabled	Controls Cisco Discovery Protocol on the PC port of the phone.

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

Field Name	Field Type or Choices	Default	Description and Usage Guidelines
SSH Access	Disabled Enabled	Disabled	Controls the access to the SSH daemon through port 22. Leaving port 22 open leaves the phone vulnerable to Denial of Service (DoS) attacks.
Incoming Call Toast Timer	Integer 3, 4, 5, 6, 7, 8, 9, 10, 15, 30, 60 seconds	5	Gives the time, in seconds, that the toast displays. The time includes the fade-in and fade-out times for the window.
Line Key Barge	cBarge Turn on Softkey Barge Off	cBarge	Controls the ability for a user to join a nonprivate call on a shared phone line. • cBarge—Enables a user to add another person to a call. The call automatically converts to a conference, allowing the user and other parties to access conference features. • Turn on Softkey—Enables a user to conference into a call on a shared line using cBarge. • Barge—Enables a user to add another user to a call but does not convert the call into a conference. • Off—Disables barge. A new call initiates when the user presses the line key.
Ring Locale	Default Japan	Default	Controls the ringing pattern.
TLS Resumption Timer	Integer 0–3600 seconds	3600	Controls the ability to resume a TLS session without repeating the entire TLS authentication process. If the field is set to 0, then the TLS session resumption is disabled.
FIPS Mode	Disabled Enabled	Disabled	Enables or disables the Federal Information Processing Standards (FIPS) mode on the phone.
HOLD/RESUME Key	HOLD/RESUME Key HOLD Key	HOLD/RESUME Key	Controls the text for the **Hold** softkey. • HOLD/RESUME Key—The softkey displays **Hold/Resume**. • HOLD Key—The softkey displays **Hold**.
Record Call Log from Shared Line	Disabled Enabled	Disabled	Specifies whether to record a shared line call in the call log.
Minimum Ring Volume	0-Silent Volume level 1–15	0-Silent	Controls the minimum ring volume for the phone. You can set a phone so that the ringer cannot be turned off.

Field Name	Field Type or Choices	Default	Description and Usage Guidelines
Peer Firmware Sharing	Disabled Enabled	Enabled	Allows the phone to find other phones of the same model on the subnet and share updated firmware files. If the phone has a new firmware load, it can share that load with the other phones. If one of the other phones has a new firmware load, the phone can download the firmware from the other phone, instead of from the TFTP server. Peer firmware sharing: • Limits congestion on TFTP transfers to centralized remove TFTP servers. • Eliminates the need to manually control firmware upgrades. • Reduces phone downtime during upgrades when large numbers of phones are reset simultaneously. • Helps with firmware upgrades in branch or remote office deployment scenarios that run over bandwidth-limited WAN links.
Load Server	String of up to 256 characters		Identifies the alternate IPv4 server that the phone uses to obtain firmware loads and upgrades. The format for the address is: `address:<port>@@base=<0-7>;pfs=<0-1>`
IPv6 Load Server	String of up to 256 characters		Identifies the alternate IPv6-only server that the phone uses to obtain firmware loads and upgrades. The format for the address is: `[address]:<port>@@base=<0-7>;pfs=<0-1>`
Wideband Headset UI Control	Disabled Enabled	Enabled	Allows the user to use the wideband codec for an analog headset.
Wideband Headset	Disabled Enabled	Enabled	Enables or disables the use of a Wideband Headset on the phone. Used in conjunction with User Control Wideband Headset. For more information, see Set Up Wideband Codec, on page 85

Field Name	Field Type or Choices	Default	Description and Usage Guidelines
Detect Unified CM Connection Failure	Normal Delayed	Normal	Determines the sensitivity that the phone has for detecting a connection failure to Cisco Unified Communications Manager (Unified CM), which is the first step before device failover to a backup Unified CM/SRST occurs. • Normal—Detection of a Unified CM connection failure occurs at the standard system rate. Choose this value for faster recognition of a Unified CM connection failure. • Delayed—Detection of a Unified CM connection failover occurs approximately four times slower than Normal. Choose this value if you prefer failover to be delayed slightly to give the connection the opportunity to reestablish The precise time difference between Normal and Delayed connection failure detection depends on many variables that are constantly changing.
Special Requirement ID	String		Controls custom features from Engineering Special (ES) loads.
Console Access	Disabled Enabled	Disabled	Specifies whether the serial console is enabled or disabled.
Actionable Incoming Call Alert	Disabled Show for all Incoming Call Show for Invisible Incoming Call	Show for all Incoming Call	Controls the type of incoming call alert that displays on the phone screen. • Disabled—The actionable incoming call alert is disabled and the user sees the traditional incoming call pop-up alert. • 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.
Energy Efficient Ethernet(EEE): PC Port	Disabled Enabled	Disabled	Controls EEE on the PC port.
Energy Efficient Ethernet(EEE): SW Port	Disabled Enabled	Disabled	Controls EEE on the SW port.

Field Name	Field Type or Choices	Default	Description and Usage Guidelines
User Credentials Persist for Expressway Sign in	Disabled Enabled	Disabled	Controls if the phone stores the user's sign-in credentials. When disabled, the user always sees the prompt to sign into the Expressway server for Mobile and Remote Access (MRA). If you would like to make it easier for users to log in, you enable this field so that the Expressway login credentials are persistent. The user then only has to enter their login credentials the first time. Any time after that (when the phone is powered on off-premise), the login information is prepopulated on the Sign-in screen. For more information, see the Mobile and Remote Access Through Expressway, on page 139.
HTPS Server	HTTP and HTTPS enabled HTTPS only	HTTP and HTTPS enabled	Controls the type of communication to the phone. If you select HTTPS only, phone communication is more secure.
Customer support upload URL	String, up to 256 characters		Provides the URL for the Problem Report Tool (PRT). If you deploy devices with Mobile and Remote Access through Expressway, you must also add the PRT server address to the HTTP Server Allow list on the Expressway server. For more information, see the Mobile and Remote Access Through Expressway, on page 139.
Recents Softkey	Disabled Enabled	Enabled	Controls the display of the Recents softkey on the phone.
Admin Configurable Ringer	Disabled Chirp1 Chirp2	Disabled	Controls the ringtone and the ability for users to set the ringtone. • When set to **Disabled**, users can configure the default ringtone on their phones. • For all other values, users cannot change the ringtone. The **Set** softkey does not display in the **Ringtone** menu.
Customer Support Use			Reserved for Cisco TAC.
Disable TLS Ciphers	See Disable Transport Layer Security Ciphers, on page 124.	None	Disables the selected TLS cipher. Disable more than one cipher suite by selecting and holding the **Ctrl** key on your computer keyboard.

Note Codec negotiation involves two steps:

1. The phone advertises the supported codec to the Cisco Unified Communications Manager. Not all endpoints support the same set of codecs.
2. When the Cisco Unified Communications Manager gets the list of supported codecs from all phones involved in the call attempt, it chooses a commonly supported codec based on various factors, including the region pair setting.

Feature Configuration Best Practices

You can set up the phone features to suit your users' needs. But we have some recommendations for certain situations and deployments that might help you.

High Call Volume Environments

In a high call volume environment, we recommend that you set up some features in a specific way.

Field	Administration Area	Recommended Setting
Always Use Prime Line	Device Information	Off or On For more information, see Field: Always Use Prime Line, on page 124.
Actionable Incoming Call Alert	Product Specific Configuration Layout	Show for all Incoming Call
Show All Calls on Primary Line	Product Specific Configuration Layout	Enabled
Revert to All Calls	Product Specific Configuration Layout	Enabled

Multiline Environments

In a multiline environment, we recommend that you set up some features in a specific way.

Field	Administration Area	Recommended Setting
Always Use Prime Line	Device Information	Off For more information, see Field: Always Use Prime Line, on page 124.
Actionable Incoming Call Alert	Product Specific Configuration Layout	Show for all Incoming Call

Field	Administration Area	Recommended Setting
Show All Calls on Primary Line	Product Specific Configuration Layout	Enabled
Revert to All Calls	Product Specific Configuration Layout	Enabled

Field: Always Use Prime Line

This field specifies whether the primary line on an IP phone is chosen when a user goes off-hook. If this parameter is set to True, when a phone goes off-hook, the primary line is chosen and becomes the active line. Even if a call rings on the second line of the user, when the phone goes off-hook, it makes only the first line active. It does not answer the inbound call on the second line. In this case, the user must choose the second line to answer the call. The default value is set to False.

The purpose of the Always Use Prime Line field is very similar to the combination of Show All Calls on the Primary Line and Revert to All Calls when both of those two features are enabled. However, the main difference is that when Always Use Prime Line is enabled, inbound calls are not answered on the second line. Only dial tone is heard on the prime line. There are certain high call volume environments where this is the desired user experience. In general, it is best to leave this field disabled except for high call volume environments that require this feature.

Disable Transport Layer Security Ciphers

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

None is the default setting.

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

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

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

Enable Call History for Shared Line

Allows you to view your shared line activity in the Call History. This feature:

- Logs missed calls for a shared line.
- Logs all answered and placed calls for a shared line.

Before you begin

Disable Privacy before you enable Call History for Shared Line. Otherwise Call History doesn't display the calls other users answer.

Procedure

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

Step 2 Locate the phone to be configured.

Step 3 Navigate to the Record Call Log from Shared Line drop-down in the Product Specific Configuration area.

Step 4 Select **Enabled** from the drop-down list.

Step 5 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.

Note The Cisco IP Phone 7811 does not support Power Save.

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.

For more information, see Product Specific Configuration, on page 109

Procedure

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

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

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

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

Table 28: PowerSave Configuration Fields

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

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

Step 4 Select **Save**.

Step 5 Select **Apply Config**.

Step 6 Restart the phone.

Schedule EnergyWise on Cisco IP Phone

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

Note The Cisco IP Phone 7811 does not support Power Save Plus.

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.

For more information, see Product Specific Configuration, on page 109

Procedure

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

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

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

- Enable Power Save Plus
- Phone On Time

- Phone Off Time
- Phone Off Idle Timeout
- Enable Audible Alert
- EnergyWise Domain
- EnergyWise Secret
- Allow EnergyWise Overrides

Table 29: EnergyWise Configuration Fields

Field	Description
Enable Power Save Plus	Selects the schedule of days for which the phone powers off. Select multiple days by pressing and holding the Control key while clicking on the days for the schedule. By default, no days are selected. When Enable Power Save Plus is checked, you receive a message that warns about emergency (e911) concerns. **Caution** While Power Save Plus Mode (the "Mode") is in effect, endpoints that are configured for the mode are disabled for emergency calling and from receiving inbound calls. By selecting this mode, you agree to the following: (i) You take full responsibility for providing alternate methods for emergency calling and receiving calls while the mode is in effect; (ii) Cisco has no liability in connection with your selection of the mode and all liability in connection with enabling the mode is your responsibility; and (iii) You fully inform users of the effects of the mode on calls, calling and otherwise. **Note** To disable Power Save Plus, you must uncheck the Allow EnergyWise Overrides check box. If the Allow EnergyWise Overrides remains checked but no days are selected in the Enable Power Save Plus field, Power Save Plus is not disabled.
Phone On Time	Determines when the phone automatically turns on for the days that are in the Enable Power Save Plus field. Enter the time in this field in 24-hour format, where 00:00 is midnight. For example, to automatically power up the phone at 07:00 a.m. (0700), enter 07:00. To power up the phone at 02:00 p.m. (1400), enter 14:00. The default value is blank, which means 00:00.

Field	Description
Phone Off Time	The time of day that the phone powers down for the days that are selected in the Enable Power Save Plus field. If the Phone On Time and the Phone Off Time fields contain the same value, the phone does not power down. Enter the time in this field in 24-hour format, where 00:00 is midnight. For example, to automatically power down the phone at 7:00 a.m. (0700), enter 7:00. To power down the phone at 2:00 p.m. (1400), enter 14:00. The default value is blank, which means 00:00. **Note** The Phone On Time must be at least 20 minutes later than the Phone Off Time. For example, if the Phone Off Time is 7:00, the Phone On Time must be no earlier than 7:20.
Phone Off Idle Timeout	The length of time that the phone must be idle before the phone powers down. The timeout occurs under the following conditions: • When the phone was in Power Save Plus mode, as scheduled, and was taken out of Power Save Plus mode because the phone user pressed the **Select** key. • When the phone is repowered by the attached switch. • When the Phone Off Time is reached but the phone is in use. The range of the field is 20 to 1440 minutes. The default value is 60 minutes.
Enable Audible Alert	When enabled, instructs the phone to play an audible alert starting 10 minutes before the time that the Phone Off Time field specifies. The audible alert uses the phone ringtone, which briefly plays at specific times during the 10-minute alerting period. The alerting ringtone plays at the user-designated volume level. The audible alert schedule is: • At 10 minutes before power down, play the ringtone four times. • At 7 minutes before power down, play the ringtone four times. • At 4 minutes before power down, play the ringtone four times. • At 30 seconds before power down, play the ringtone 15 times or until the phone powers off. This check box applies only if the Enable Power Save Plus list box has one or more days selected.
EnergyWise Domain	The EnergyWise domain that the phone is in. The maximum length of this field is 127 characters.
EnergyWise Secret	The security secret password that is used to communicate with the endpoints in the EnergyWise domain. The maximum length of this field is 127 characters.

Field	Description
Allow EnergyWise Overrides	This check box determines whether you allow the EnergyWise domain controller policy to send power level updates to the phones. The following conditions apply: • One or more days must be selected in the Enable Power Save Plus field. • The settings in Cisco Unified Communications Manager Administration take effect on schedule even if EnergyWise sends an override. For example, assuming the Phone Off Time is set to 22:00 (10:00 p.m.), the value in the Phone On Time field is 06:00 (6:00 a.m.), and the Enable Power Save Plus has one or more days selected. • If EnergyWise directs the phone to turn off at 20:00 (8:00 p.m.), that directive remains in effect (assuming no phone user intervention occurs) until the configured Phone On Time at 6:00 a.m. • At 6:00 a.m., the phone turns on and resumes receiving the power level changes from the settings in Unified Communications Manager Administration. • To change the power level on the phone again, EnergyWise must reissue a new power level change command. **Note** To disable Power Save Plus, you must uncheck the Allow EnergyWise Overrides check box. If the Allow EnergyWise Overrides remains checked but no days are selected in the Enable Power Save Plus field, Power Save Plus is not disabled.

Step 4 Select **Save**.

Step 5 Select **Apply Config**.

Step 6 Restart the phone.

Set up AS-SIP

Depending on how you have configured your phone system, you may be able to make priority calls using the Assured Services for SIP Lines (AS-SIP) feature.

With this feature, routine calls are placed normally. However, during an emergency, you can select a priority level that helps ensure the delivery of critical calls. Depending upon how your phone is configured, you may have to sign-in also.

When you receives a priority call, a precedence level icon displays next to the caller's name on your phone.

Procedure

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

Step 2 Select a profile.

Step 3 Set the Is Assured SIP Service Enabled check box.

This setting provides specific Assured Service behavior that affects services such as Conference factory and SRTP.

Step 4 Enable MLPP Authorization for a device by checking the MLPP User Authorization check box.

When the MLPP User Authorization check box is enabled, the system challenges the AS-SIP phone for the user's credentials when a precedence call is made.

Step 5 Set the Resource Priority namespace.

An AS-SIP phone is associated with a single Resource Priority namespace.

If <*None*> is left as the namespace in the SIP profile, then the default namespace is used.

All devices using this profile must be restarted.

Step 6 Select **Apply**.

Step 7 Choose **Device** > **Phone**.

Step 8 Locate the phone that you are setting up.

Step 9 Navigate to the MLPP section and set the following fields:

- MLPP Indication:
  - Set the MLPP Indication to **On** to enable MLPP regardless of the enterprise or common config settings.
  - Set the MLPP Indication to **Default** and MLPP is enabled for a device at the common device config or enterprise parameter levels.
  - When MLPP Indication is set to **Off**, MLPP is disabled for the device regardless of the common device or enterprise parameter configuration.
- MLPP Preemption: Determines whether preemption for reuse can be performed on the device. This type of preemption is used to remove an existing call and offer a higher precedence call to the user of the device.
  - When set to **Disabled**, only preemption 'not for reuse' can be performed on the device. This type of preemption occurs when the user is not the called party but is in a call with the called party or is using a preempted network resource. For example, a trunk channel or reserved bandwidth allocation.
  - When set to **Forceful**, preempt for reuse is enabled. Existing calls may be preempted to offer a higher precedence call to the user.
  - When set to **Default**, the setting from the common configuration or enterprise level is used.

Step 10 Choose **User Management** > **End User** and select a user.

Step 11 Navigate to the MLPP Authorization section and configure MLPP Authorization for a user.

The MLPP User Identification number must be composed of 6 to 20 numeric characters.

The MLPP Password must be composed of 4 to 20 numeric (0-9) characters

The Precedence Authorization level can be set to any standard precedence level from Routine to Executive Override

Step 12 Select **Save**.

Step 13 Set up the MLPP DSCP for an End User.

The DSCP values for video streams can be configured for each precedence level in the QoS section of the Service Parameters. All DSCP values include the decimal value in the setting.

Step 14 To add a third-party AS-SIP phone, choose **Device** > **Phone** > **Add New**

The phone Add list displays the third-party AS-SIP phone as an available choice.

The device configuration fields are the same as those for Cisco phones.

Set Up Do Not Disturb

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

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

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

Procedure

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

Step 2 Locate the phone to be configured.

Step 3 Set the following parameters.

- Do Not Disturb: This check box allows you to enable DND on the phone.
- DND Option: Ring Off, Call Reject, or Use Common Phone Profile Setting.

  Do not choose Call Reject if you want priority (MLPP) calls to ring this phone when DND is turned on.
- DND Incoming Call Alert: Choose the type of alert, if any, to play on a phone for incoming calls when DND is active.

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

Step 4 Select **Save**.

Related Topics

Cisco Unified Communications Manager Documentation, on page xv

Enable Agent Greeting

The Agent Greeting feature allows an agent to create and update a prerecorded greeting that plays at the beginning of a call, such as a customer call, before the agent begins the conversation with the caller. The agent can prerecord a single greeting or multiple greetings, as needed, and create and update the greetings.

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

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

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

Procedure

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

Step 2 Locate the IP phone that you want to configure.

Step 3 Scroll to the Device Information Layout pane and set **Built In Bridge** to On or Default.

Step 4 Select **Save**.

Step 5 Check the setting of the bridge:

a) Choose **System** > **Service Parameters**.
b) Select the appropriate Server and Service.
c) Scroll to the Clusterwide Parameters (Device - Phone) pane and set **Builtin Bridge Enable** to On.
d) Select **Save**.

Related Topics

Cisco Unified Communications Manager Documentation, on page xv

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 information in the documentation for your particular Cisco Unified Communications Manager release.

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**.

Related Topics

Cisco Unified Communications Manager Documentation, on page xv

Set Up Call Forward Notification

You can control the call forward settings.

Procedure

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

Step 2 Locate the phone to be set up.

Step 3 Configure the Call Forward Notification fields.

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

Field	Description
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**.

Enable BLF for Call Lists

Procedure

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

Step 2 From the BLF for Call Lists drop-down list box, choose the applicable profile.

By default, the feature is disabled.

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

a. Device Configuration window settings

b. Common Phone Profile window settings

c. Enterprise Phone Configuration window settings

Step 3 Select **Save**.

Enable Device Invoked Recording

Configure the Device Invoked Recording feature from Cisco Unified Communications Manager Administration. For more information, see the documentation for your particular Cisco Unified Communications Manager release.

Procedure

Step 1 Set the IP Phone Built In Bridge parameter to **On**.

Step 2 In the Line Configuration page, set Recording Option to **Selective Call Recording Enabled** and select the appropriate Recording profile.

Related Topics

Cisco Unified Communications Manager Documentation, on page xv

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 30: UCR 2008 Parameter Location

Parameter	Administration Path
FIPS Mode	**Device** > **Device Settings** > **Common Phone Profile**
	System > **Enterprise Phone Configuration**
	Device > **Phones**
SSH Access	**Device** > **Phone**
	Device > **Device Settings** > **Common Phone Profile**
Web Access	**Device** > **Phone**
	System > **Enterprise Phone Configuration**
	Device > **Device Settings** > **Common Phone Profile**
80-bit SRTCP	**Device** > **Device Settings** > **Common Phone Profile**
	System > **Enterprise Phone Configuration**
IP Addressing Mode	**Device** > **Device Settings** > **Common Device Configuration**
IP Addressing Mode Preference for Signaling	**Device** > **Device Settings** > **Common Device Configuration**

Set Up UCR 2008 in Common Device Configuration

Use this procedure to set the following UCR 2008 parameters:

- IP Addressing Mode
- IP Addressing Mode Preference for Signaling

Procedure

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

Step 2 Set the IP Addressing Mode parameter.

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

Step 4 Select **Save**.

Set Up UCR 2008 in Common Phone Profile

Use this procedure to set the following UCR 2008 parameters:

- FIPS Mode
- SSH Access
- 80-bit SRTCP
- Web Access

Procedure

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

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

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

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

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

Step 6 Select **Save**.

Set Up UCR 2008 in Enterprise Phone Configuration

Use this procedure to set the following UCR 2008 parameters:

- FIPS Mode
- 80-bit SRTCP
- Web Access

Procedure

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

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

Step 3 Set the 80-bit SRTCP parameter to **Enabled**.

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

Step 5 Select **Save**.

Set Up UCR 2008 in Phone

Use this procedure to set the following UCR 2008 parameters:

- FIPS Mode
- SSH Access
- Web Access

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Device** > **Phone**.
Step 2 Set the SSH Access parameter to **Disabled**.
Step 3 Set the FIPS Mode parameter to **Enabled**.
Step 4 Set the Web Access parameter to **Disabled**.
Step 5 Select **Save**.

Set Up RTP/sRTP Port Range

You configure the Real-Time Transport Protocol (RTP) and secure Real-Time Transport Protocol (sRTP) port values in the SIP profile. RTP and sRTP port values range from 2048 to 65535, with a default range of 16384 to 32764. Some port values within the RTP and sRTP port range are designated for other phone services. You cannot configure these ports for RTP and sRTP.

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

Procedure

Step 1 Select **Device** > **Device Settings** > **SIP Profile**
Step 2 Choose the search criteria to use and click **Find**.
Step 3 Select the profile to modify.
Step 4 Set the Start Media Port and Stop Media Port to contain the start and end of the port range.

The following list identifies the UDP ports that are used for other phone services and thus not available for RTP and sRTP use:

port 4051

used for the Peer Firmware Sharing (PFS) feature

port 5060

used for SIP over UDP transport

port range 2048 to 49150

Do not configure the Stop Media Port to a value over 49150.

Step 5 Click **Save**.

Step 6 Click **Apply Config**.

Related Topics

Cisco Unified Communications Manager Documentation, on page xv

Mobile and Remote Access Through Expressway

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

The list of CA certificates embedded in the phone firmware is available at http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-7800-series/products-technical-reference-list.html.

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

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

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

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

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

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

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

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

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

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

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

Deployment Scenarios

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

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

Media Paths and Interactive Connectivity Establishment

You can deploy Interactive Connectivity Establishment (ICE) to improve the reliability of Mobile and Remote Access (MRA) calls that cross a firewall or Network Address Translation (NAT). ICE is an optional deployment that uses Serial Tunneling and Traversal Using Relays around NAT services to select the best media path for a call.

Secondary Turn Server and Turn Server Failover is not supported.

For more information about MRA and ICE, see *System Configuration Guide for Cisco Unified Communications Manager, Release 12.0(1)* or later. You can also find additional information in the Internet Engineering Task Force (IETF) Request for Comment documents:

- *Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)*(RFC 5766)
- *Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols* (RFC 5245)

Phone Features Available for Mobile and Remote Access Through Expressway

Mobile and Remote Access Through Expressway provides secure VPN-less access to collaboration services for Cisco mobile and remote users. But to preserve network security, it limits access to some phone features.

The following list shows the phone features available with Mobile and Remote Access Through Expressway.

Table 31: Feature Support and Mobile and Remote Access Through Expressway

Phone Feature	Phone Firmware Release
Abbreviated Dialing	10.3(1) and later
Answer Oldest	11.5(1)SR1 and later
Assisted Directed Call Park	10.3(1) and later
Auto Answer	11.5(1)SR1 and later
Barge and cBarge	11.5(1)SR1 and later
Busy Lamp Field (BLF)	10.3(1) and later
Busy Lamp Field (BLF) Pickup	10.3(1) and later
Busy Lamp Field (BLF) Speed Dial	10.3(1) and later
Call Back	10.3(1) and later
Call Forward	10.3(1) and later
Call Forward Notification	10.3(1) and later
Call Park	10.3(1) and later
Call Pickup	10.3(1) and later
Cisco Unified Serviceability	11.5(1)SR1 and later
Client Access License (CAL)	11.5(1)SR1 and later
Conference	10.3(1) and later
Conference List / Remove Participant	11.5(1)SR1 and later

Phone Feature	Phone Firmware Release
Corporate Directory	11.5(1)SR1 and later
CTI Applications (CTI Controlled)	11.5(1)SR1 and later
Directed Call Park	10.3(1) and later
Distinctive Ring	11.5(1)SR1 and later
Divert	10.3(1) and later
Divert	10.3(1) and later
Forced Access Codes and Client Matter Codes	11.5(1)SR1 and later
Group Call Pickup	10.3(1) and later
Hold/Resume	10.3(1) and later
Hold Reversion	10.3(1) and later
Immediate Divert	10.3(1) and later
Join	10.3(1) and later
Malicious Caller Identification (MCID)	11.5(1)SR1 and later
Meet Me Conference	10.3(1) and later
Message Waiting Indicator	10.3(1) and later
Mobile Connect	10.3(1) and later
Mobile Voice Access	10.3(1) and later
Multilevel Precedence and Preemption (MLPP)	11.5(1)SR1 and later
Multiline	11.5(1)SR1 and later
Music On Hold	10.3(1) and later
Mute	10.3(1) and later
Network profiles (Automatic)	11.5(1)SR1 and later
Off-hook Dialing	10.3(1) and later
On-hook Dialing	10.3(1) and later
Plus Dialing	10.3(1) and later
Privacy	11.5(1)SR1 and later
Private Line Automated Ringdown (PLAR)	11.5(1)SR1 and later
Redial	10.3(1) and later

Phone Feature	Phone Firmware Release
Speed Dial (does not support a pause)	10.3(1) and later
Services URL button	11.5(1)SR1 and later
Transfer	10.3(1) and later
Uniform Resource Identifier (URI) Dialing	10.3(1) and later

Problem Report Tool

Users submit problem reports to you with the Problem Report Tool.

Note The Problem Report Tool logs are required by Cisco TAC when troubleshooting problems. The logs are cleared if you restart the phone. Collect the logs before you restart the phones.

To issue a problem report, users access the Problem Report Tool and provide the date and time that the problem occurred, and a description of the problem.

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

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

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

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

Configure a Customer Support Upload URL

You must use a server with an upload script to receive PRT files. The PRT uses an HTTP POST mechanism, with the following parameters included in the upload (utilizing multipart MIME encoding):

- devicename (example: “SEP001122334455”)
- serialno (example: “FCH12345ABC”)
- username (the username configured in Cisco Unified Communications Manager, the device owner)
- prt_file (example: “probrep-20141021-162840.tar.gz”)

A sample script is shown below. This script is provided for reference only. Cisco does not provide support for the upload script installed on a customer's server.

```
<?php

// NOTE: you may need to edit your php.ini file to allow larger
// size file uploads to work.
// Modify the setting for upload_max_filesize
// I used:  upload_max_filesize = 20M

// Retrieve the name of the uploaded file
$filename = basename($_FILES['prt_file']['name']);

// Get rid of quotes around the device name, serial number and username if they exist
$devicename = $_POST['devicename'];
$devicename = trim($devicename, "'\"");

$serialno = $_POST['serialno'];
$serialno = trim($serialno, "'\"");

$username = $_POST['username'];
$username = trim($username, "'\"");

// where to put the file
$fullfilename = "/var/prtuploads/".$filename;

// If the file upload is unsuccessful, return a 500 error and
// inform the user to try again

if(!move_uploaded_file($_FILES['prt_file']['tmp_name'], $fullfilename)) {
        header("HTTP/1.0 500 Internal Server Error");
        die("Error: You must select a file to upload.");
}

?>
```

Note The phones only support HTTP URLs.

Procedure

Step 1 Set up a server that can run your PRT upload script.

Step 2 Write a script that can handle the parameters listed above, or edit the provided sample script to suit your needs.

Step 3 Upload your script to your server.

Step 4 In Cisco Unified Communications Manager, go to the Product Specific Configuration Layout area of the individual device configuration window, Common Phone Profile window, or Enterprise Phone Configuration window.

Step 5 Check **Customer support upload URL** and enter your upload server URL.

Example:

http://example.com/prtscript.php

Step 6 Save your changes.

Set the Label for a Line

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

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

Procedure

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

Step 2 Locate the phone to be configured.

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

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

Step 5 Select **Save**.

Assured Services SIP

Assured Services SIP(AS-SIP) is a collection of features and protocols that offer a highly secure call flow for Cisco IP Phones and third-party phones. The following features are collectively known as AS-SIP:

- Multilevel Precedence and Preemption (MLPP)
- Differentiated Services Code Point (DSCP)
- Transport Layer Security (TLS) and Secure Real-time Transport Protocol (SRTP)
- Internet Protocol version 6 (IPv6)

AS-SIP is often used with Multilevel Precedence and Preemption (MLPP) to prioritize calls during an emergency. With MLPP, you assign a priority level to your outgoing calls, from level 1 (low) to level 5 (high). When you receive a call, a precedence level icon displays on the phone that shows the call priority.

To configure AS-SIP, complete the following tasks on Cisco Unified Communications Manager:

- Configure a Digest User—Configure the end user to use digest authentication for SIP requests.
- Configure SIP Phone Secure Port—Cisco Unified Communications Manager uses this port to listen to SIP phones for SIP line registrations over TLS.
- Restart Services—After configuring the secure port, restart the Cisco Unified Communications Manager and Cisco CTL Provider services. Configure SIP Profile for AS-SIP-Configure a SIP profile with SIP settings for your AS-SIP endpoints and for your SIP trunks. The phone-specific parameters are not downloaded to a third-party AS-SIP phone. They are used only by Cisco Unified Manager. Third-party phones must locally configure the same settings.
- Configure Phone Security Profile for AS-SIP—You can use the phone security profile to assign security settings such as TLS, SRTP, and digest authentication.
- Configure AS-SIP Endpoint—Configure a Cisco IP Phone or a third-party endpoint with AS-SIP support.

- Associate Device with End Use—Associate the endpoint with a user.
- Configure SIP Trunk Security Profile for AS-SIP—You can use the sip trunk security profile to assign security features such as TLS or digest authentication to a SIP trunk.
- Configure SIP Trunk for AS-SIP—Configure a SIP trunk with AS-SIP support.
- Configure AS-SIP Features—Configure additional AS-SIP features such as MLPP, TLS, V.150, and IPv6.

For detailed information about configuring AS-SIP, see the "Configure AS-SIP Endpoints" chapter, *System Configuration Guide for Cisco Unified Communications Manager*.

Multilevel Precedence and Preemption

Multilevel Precedence and Preemption (MLPP) allows you to prioritize calls during emergencies or other crisis situations. You assign a priority to your outgoing calls that range from 1 to 5. Incoming calls display an icon that shows the call priority. Authenticated users can preempt calls either to targeted stations or through fully subscribed TDM trunks.

This capability assures high-ranking personnel of communication to critical organizations and personnel.

MLPP is often used with Assured Services SIP(AS-SIP). For detailed information about configuring MLPP, see the "Configure Multilevel Precedence and Preemption" chapter, *System Configuration Guide for Cisco Unified Communications Manager*.

Migration of your Phone to a Multiplatform Phone Directly

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

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

Set Up Softkey Template

You can associate up to 18 softkeys with applications that are supported by the Cisco IP Phone. 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 the documentation for your particular Cisco Unified Communications Manager release.

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.

Table 32: Configurable Softkeys

Feature	Configurable softkeys in the Softkey Template configuration	Support status	Notes
Answer	Answer (Answer)	Yes	-
Barge	Barge (Barge)	No	Cisco IP Phone 7811, 7821, 7841, and 7861 support cBarge only.
Call Back	Call Back (CallBack)	Yes	Configure as a programmable line key or as a softkey.
Call Forward All	Forward All (cfwdAll)	Yes	Phone displays `Fwd ALL` or `Fwd Off`.
Call Park	Call Park (Park)	Yes	Configure as a programmable line key or as a softkey.
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 (Conf)	Yes	Configure as a softkey only.
Conference List	Details	Yes	Phone displays Details.
Divert	ImmediateDivert (iDivert)	Yes	Phone displays Divert. Starting with Firmware Release 10.3(1), the phone displays Decline for the softkey.
Do Not Disturb	Toggle Do Not Disturb (DND)	Yes	Configure as a programmable line button or softkey.
End Call	End Call (EndCall)	Yes	
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 line button or softkey.
Join	Join (Join)	No	
Malicious Call Identification	Toggle Malicious Call Identification (MCID)	Yes	Configure as a programmable feature button or softkey.
Meet Me	Meet Me (MeetMe)	Yes	Configure as a programmable feature button or softkey.

Feature	Configurable softkeys in the Softkey Template configuration	Support status	Notes
Mobile Connect	Mobility (Mobility)	Yes	Configure as a programmable feature button or softkey.
New Call	New Call (NewCall)	Yes	Phone displays `New Call`.
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.
Recents	Recents	Yes	Enables/Disables the softkey.
Redial	Redial (Redial)	Yes	-
Remove Last Conference Participant	Remove Last Conference Participant (Remove)	Yes	Phone displays `Remove` when a participant is selected.
Resume	Resume (Resume)	Yes	Resume is a dedicated button.
Speed Dial	Abbreviated Dial (AbbrDial)	Yes	Phone displays `SpeedDial`.
Transfer	Direct Transfer (DirTrfr)	Yes	This feature is supported as a soft key or a dedicated button.
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, template, and modification

Step 6 Select **Apply Config** to apply the template to the phones.

Related Topics

Cisco Unified Communications Manager Documentation, on page xv

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 and configuring line buttons, see the documentation for your particular Cisco Unified Communications Manager release.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Device** > **Device Settings** > **Phone Button Template**.

Step 2 Click **Find**.

Step 3 Select the phone model.

Step 4 Select **Copy**, enter a name for the new template, and then select **Save**.

The Phone Button Template Configuration window opens.

Step 5 Identify the button that you would like to assign, and select **Service URL** from the Features drop-down list that associates with the line.

Step 6 Select **Save** to create a new phone button template that uses the service URL.

Step 7 Choose **Device** > **Phone** and open the Phone Configuration window for the phone.

Step 8 Select the new phone button template from the Phone Button Template drop-down list.

Step 9 Select **Save** to store the change and then select **Apply Config** to implement the change.

The phone user can now access the Self Care Portal and associate the service with a button on the phone.

Related Topics

Cisco Unified Communications Manager Documentation, on page xv

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

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: 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**.

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.

Related Topics

Cisco Unified Communications Manager Documentation, on page xv

Headset Management on Older Versions of Cisco Unified Communications Manager

If you have a version of Cisco Unified Communications Manager older than 12.5(1)SU1, you can remotely configure your Cisco headset settings for use with on-premises phones.

Remote headset configuration on Cisco Unified Communication Manager version 10.5(2), 11.0(1), 11.5(1), 12.0(1), and 12.5(1) requires you to download a file from the Cisco Software Download website, edit the file, and then upload the file on the Cisco Unified Communications Manager TFTP server. The file is a JavaScript Object Notification (JSON) file. The updated headset configuration is applied to the enterprise headsets over a 10 to 30-minute time frame to prevent a traffic backlog on the TFTP server.

Note You can manage and configure headsets through Cisco Unified Communications Manager Administration version 11.5(1)SU7.

Note the following as you work with the JSON file:

- The settings aren't applied if you are missing a bracket or brackets in the code. Use an online tool such as JSON Formatter and check the format.
- Set the **updatedTime** setting to the current epoch time or the configuration is not applied. Alternatively, you can increase the **updatedTime** value by +1 to make it larger than the previous version.
- Do not change the parameter name or the setting will not be applied.

For more information on the TFTP service, see the "Manage Device Firmware" chapter of the *Administration Guide for Cisco Unified Communications Manager and IM and Presence Service*.

Upgrade your phones to the latest firmware release before you apply the `defaultheadsetconfig.json` file. The following table describes the default settings you can adjust with the JSON file.

Download the Default Headset Configuration File

Before configuring the headset parameters remotely, you must download the latest JavaScript Object Notation (JSON) sample file.

Procedure

Step 1 Go to the following URL: https://software.cisco.com/download/home/286320550.

Step 2 Choose **Headsets 500 Series**.

Step 3 Select your headset series.

Step 4 Choose a release folder and select the zip file.

Step 5 Click the **Download** or **Add to cart** button, and follow the prompts.

Step 6 Unzip the file to a directory on your PC.

What to do next

Modify the Default Headset Configuration File, on page 152

Modify the Default Headset Configuration File

Note the following as you work with the JavaScript Object Notation (JSON) file:

- The settings aren't applied if you are missing a bracket or brackets in the code. Use an online tool such as JSON Formatter and check the format.
- Set the "**updatedTime**" setting to the current epoch time or the configuration is not applied.
- Confirm that **firmwareName** is `LATEST` or the configurations will not be applied.
- Do not change a parameter name or the setting will not be applied.

Procedure

Step 1 Open the `defaultheadsetconfig.json` file with a text editor.

Step 2 Edit the **updatedTime** and the headset parameter values you wish to modify.

A sample script is shown below. This script is provided for reference only. Use it as a guide as you configure your headset parameters. Use the JSON file that was included with your firmware load.

```
{
  "headsetConfig": {
    "templateConfiguration": {
      "configTemplateVersion": "1",
      "updatedTime": 1537299896,
      "reportId": 3,
      "modelSpecificSettings": [
        {
          "modelSeries": "530",
          "models": [
            "520",
            "521",
            "522",
            "530",
            "531",
            "532"
          ],
          "modelFirmware": [
            {
              "firmwareName": "LATEST",
              "latest": true,
              "firmwareParams": [
                {
                  "name": "Speaker Volume",
                  "access": "Both",
                  "usageId": 32,
                  "value": 7
                },
                {
                  "name": "Microphone Gain",
                  "access": "Both",
                  "usageId": 33,
                  "value": 2
```

```
        },
        {
          "name": "Sidetone",
          "access": "Both",
          "usageId": 34,
          "value": 1
        },
        {
          "name": "Equalizer",
          "access": "Both",
          "usageId": 35,
          "value": 3
        }
      ]
    }
  ]
},
{
  "modelSeries": "560",
  "models": [
    "560",
    "561",
    "562"
  ],
  "modelFirmware": [
    {
      "firmwareName": "LATEST",
      "latest": true,
      "firmwareParams": [
        {
          "name": "Speaker Volume",
          "access": "Both",
          "usageId": 32,
          "value": 7
        },
        {
          "name": "Microphone Gain",
          "access": "Both",
          "usageId": 33,
          "value": 2
        },
        {
          "name": "Sidetone",
          "access": "Both",
          "usageId": 34,
          "value": 1
        },
        {
          "name": "Equalizer",
          "access": "Both",
          "usageId": 35,
          "value": 3
        },
        {
          "name": "Audio Bandwidth",
          "access": "Admin",
          "usageId": 36,
          "value": 0
        },
        {
          "name": "Bluetooth",
          "access": "Admin",
          "usageId": 39,
          "value": 0
```

```
                },
                {
                  "name": "DECT Radio Range",
                  "access": "Admin",
                  "usageId": 37,
                  "value": 0
                }
                {
                   "name": "Conference",
                  "access": "Admin",
                  "usageId": 41,
                  "value": 0
              ]
            }
          ]
        }
      ]
    }
  }
}
```

Step 3 Save the `defaultheadsetconfig.json`.

What to do next

Install the default configuration file.

Install the Default Configuration File on Cisco Unified Communications Manager

After you edit the `defaultheadsetconfig.json` file, install it on Cisco Unified Communications Manager using the TFTP File Management tool.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Software Upgrades** > **TFTP File Management**.

Step 2 Select **Upload File**.

Step 3 Select **Choose File** and navigate to the `defaultheadsetconfig.json` file.

Step 4 Select **Upload File**.

Step 5 Click **Close**.

Restart the Cisco TFTP Server

After you upload the `defaultheadsetconfig.json` file to the TFTP directory, restart the Cisco TFTP server and reset the phones. After about 10–15 minutes, the download process begins and the new configurations are applied to the headsets. It takes an additional 10 to 30 minutes for the settings to be applied.

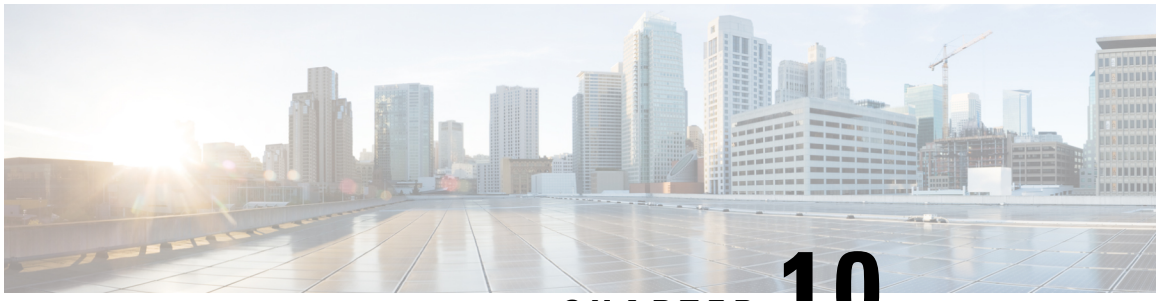
Procedure

Step 1 Log in to Cisco Unified Serviceability and choose **Tools** > **Control Center - Feature Services**.

Step 2 From the **Server** drop-down list box, choose the server on which the Cisco TFTP service is running.

Step 3 Click the radio button that corresponds to the **Cisco TFTP** service.

Step 4 Click **Restart**.



CHAPTER 10

Corporate and Personal Directory Setup

- Corporate Directory Setup, on page 157
- Personal Directory Setup, on page 157
- User Personal Directory Entries Setup, on page 158

Corporate Directory Setup

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

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

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

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

Related Topics

Cisco Unified Communications Manager Documentation, on page xv

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 CiscoIP 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 158 and Set Up Synchronizer, on page 159.

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

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

User Personal Directory Entries Setup

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

- Self Care Portal: Make sure that users know how to access their Self Care Portal. See Set Up User Access to the Self Care Portal, on page 69 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 158.

Note The Cisco IP Phone Address Book Synchronizer is only supported on unsupported versions of Windows (for example, Windows XP and earlier). The tool is not supported on newer versions of Windows. In future, it will be removed from the Cisco Unified Communications Manager plug-ins list.

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 159 to all users who require this application.

Cisco IP Phone Address Book Synchronizer Deployment

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

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

Install Synchronizer

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

Procedure

Step 1 Get the Cisco IP Phone Address Book Synchronizer installer file from your system administrator.
Step 2 Double-click the TabSyncInstall.exe file that your administrator provided.
Step 3 Select **Run**.
Step 4 Select **Next**.
Step 5 Read the license agreement information, and select the **I Accept**. Select **Next**.
Step 6 Choose the directory in which you want to install the application and select **Next**.
Step 7 Select **Install**.
Step 8 Select **Finish**.
Step 9 To complete the process, follow the steps in Set Up Synchronizer, on page 159.

Set Up Synchronizer

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

Procedure

Step 1 Open the Cisco IP Phone Address Book Synchronizer.

If you accepted the default installation directory, you can open the application by choosing **Start** > **All Programs** > **Cisco Systems** > **TabSync**.

Step 2 To configure user information, select **User**.
Step 3 Enter the Cisco IP Phone user name and password and select **OK**.

Step 4 To configure Cisco Unified Communications Manager server information, select **Server**.

Step 5 Enter the IP address or host name and the port number of the Cisco Unified Communications Manager server and select **OK**.

If you do not have this information, contact your system administrator.

Step 6 To start the directory synchronization process, select **Synchronize**.

The Synchronization Status window provides the status of the address book synchronization. If you chose the user intervention for duplicate entries rule and you have duplicate address book entries, the Duplicate Selection window displays.

Step 7 Choose the entry that you want to include in your Personal Address Book and select **OK**.

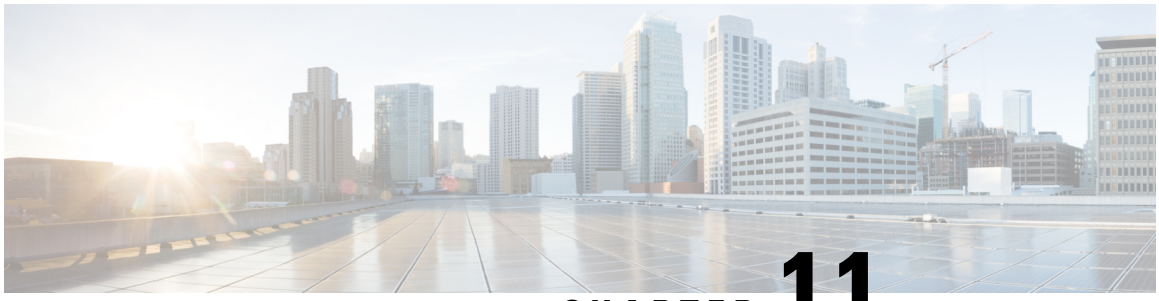
Step 8 When synchronization is complete, select **Exit** to close the Cisco Unified CallManager Address Book Synchronizer.

Step 9 To verify whether the synchronization worked, sign in to your Self Care Portal and choose **Personal Address Book**. The users from your Windows address book should be listed.

PART IV

Cisco IP Phone Troubleshooting

- Monitoring Phone Systems, on page 163
- Troubleshooting, on page 193
- Maintenance, on page 211
- International User Support, on page 217



CHAPTER 11

Monitoring Phone Systems

- Monitoring Phone Systems Overview, on page 163
- Cisco IP Phone Status, on page 163
- Cisco IP Phone Web Page, on page 176
- Request Information from the Phone in XML, on page 189

Monitoring Phone Systems Overview

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

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

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

Cisco IP Phone Status

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

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

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

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

Display the Phone Information Window

Procedure

Step 1 Press **Settings** softkey.

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 .

Display Status Menu

Procedure

Step 1 To display the Status menu, press **Applications** .

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

Step 3 To exit the Status menu, press **Back** .

Display Status Messages Window

Procedure

Step 1 Press **Applications** .

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

Step 3 To remove current status messages, press **Clear**.

Step 4 To exit the Status menu, press **Back** .

Related Topics

Phone Displays Error Messages, on page 196

Status Messages Fields

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

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

Table 33: Status Messages on the Cisco IP Phone

Message	Description	Possible Explanation and Action
Could not acquire an IP address from DHCP	The phone has not previously obtained an IP address from a DHCP Server. This can occur when you perform an out of box or factory reset.	Confirm that the DHCP server is ava is available for the phone.
TFTP Size Error	The configuration file is too large for file system on the phone.	Power cycle the phone.
ROM Checksum Error	Downloaded software file is corrupted.	Obtain a new copy of the phone firr TFTPPath directory. You should on directory when the TFTP server softv the files may be corrupted.
Duplicate IP	Another device is using the IP address that is assigned to the phone.	If the phone has a static IP address, assigned a duplicate IP address. If you are using DHCP, check the D
Erasing CTL and ITL files	Erasing CTL or ITL file.	None. This message is informationa
Error Updating Locale	One or more localization files could not be found in the TFTP Path directory or were not valid. The locale was not changed.	From Cisco Unified Operating Syst that the following files are located v TFTP File Management: • Located in subdirectory with sa • tones.xml • Located in subdirectory with s • glyphs.xml • dictionary.xml • kate.xml

Message	Description	Possible Explanation and Action
File not found <Cfg File>	The name-based and default configuration file was not found on the TFTP Server.	The configuration file for a phone is cr added to the Cisco Unified Communica If the phone does not exist in the Cisco U Manager database, the TFTP server ge **`Not Found`** response. • Phone is not registered with Cisco U Manager. You must manually add the phone Communications Manager if you to autoregister. • If you are using DHCP, verify tha pointing to the correct TFTP serve • If you are using static IP addresses the TFTP server.
File Not Found <CTLFile.tlv>	This message displays on the phone when the Cisco Unified Communications Manager cluster is not in secure mode.	No impact; the phone can still register Communications Manager.
IP Address Released	The phone is configured to release the IP address.	The phone remains idle until it is power the DHCP address.
IPv4 DHCP Timeout	IPv4 DHCP server did not respond.	Network is busy: The errors should res the network load reduces. No network connectivity between the I the phone: Verify the network connecti IPv4 DHCP server is down: Check conf server. Errors persist: Consider assigning a sta
IPv6 DHCP Timeout	IPv6 DHCP server did not respond.	Network is busy - The errors should re the network load reduces. No network connectivity between the I the phone: Verify the network connecti IPv6 DHCP server is down: Check conf server. Errors persist: Consider assigning a sta

Message	Description	Possible Explanation and Action
IPv4 DNS Timeout	IPv4 DNS server did not respond.	Network is busy: The errors should the network load reduces. No network connectivity between t phone: Verify the network connecti IPv4 DNS server is down: Check co server.
IPv6 DNS Timeout	IPv6 DNS server did not respond.	Network is busy: The errors should the network load reduces. No network connectivity between t phone: Verify the network connecti IPv6 DNS server is down: Check co server.
DNS unknown IPv4 Host	IPv4 DNS could not resolve the name of the TFTP server or Cisco Unified Communications Manager.	Verify that the host names of the TF Communications Manager are confi Consider using IPv4 addresses rath
DNS unknown IPv6 Host	IPv6 DNS could not resolve the name of the TFTP server or Cisco Unified Communications Manager.	Verify that the host names of the TF Communications Manager are confi Consider using IPv6 addresses rath
Load Rejected HC	The application that was downloaded is not compatible with the phone hardware.	Occurs if you attempted to install a phone that did not support hardwar Check the load ID that is assigned t Unified Communications Manager, Reenter the load that displays on th
No Default Router	DHCP or static configuration did not specify a default router.	If the phone has a static IP address, is configured. If you are using DHCP, the DHCP s default router. Check the DHCP ser
No IPv4 DNS Server	A name was specified but DHCP or static IP configuration did not specify a IPv4 DNS server address.	If the phone has a static IP address, server is configured. If you are using DHCP, the DHCP s IPv4 DNS server. Check the DHCP
No IPv6 DNS Server	A name was specified but DHCP or static IP configuration did not specify a IPv6 DNS server address.	If the phone has a static IP address, server is configured. If you are using DHCP, the DHCP s IPv6 DNS server. Check the DHCP

Message	Description	Possible Explanation and Action
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 C Communications Manager, which does default. The trust list is not configured.
Phone failed to register. Cert key size is not FIPS compliant.	FIPS requires that the RSA server certificate is 2048 bits or greater.	Update the certificate.
Restart requested by Cisco Unified Communications Manager	The phone is restarting due to on a request from Cisco Unified Communications Manager.	Configuration changes were likely mad Unified Communications Manager, and 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 I to the correct TFTP server. If you are using static IP addresses, chec server.
TFTP Error	The phone does not recognize an error code that the TFTP server provided.	Contact Cisco TAC.
TFTP Timeout	TFTP server did not respond.	Network is busy: The errors should res the network load reduces. No network connectivity between the TF Verify the network connections. TFTP server is down: Check configura
Timed Out	Supplicant attempted 802.1X transaction but timed out to due the absence of an authenticator.	Authentication typically times out if 80 on the switch.

Message	Description	Possible Explanation and Action
Trust List Update Failed	Update of the CTL and ITL files failed.	Phone has CTL and ITL files install new CTL and ITL files. Possible reasons for failure: • Network failure occurred. • TFTP server was down. • The new security token that w the TFTP certificate that was u introduced, but are not availab ITL files in the phone. • Internal phone failure occurre Possible solutions: • Check network connectivity. • Check whether the TFTP serv normally. • If the Transactional Vsam Ser supported on Cisco Unified C check whether the TVS server normally. • Verify whether the security to valid. Manually delete the CTL and ITL f solutions fail; reset the phone.
Trust List Updated	The CTL file, the ITL file, or both files are updated.	None. This message is informationa
Version Error	The name of the phone load file is incorrect.	Make sure that the phone load file l
XmlDefault.cnf.xml, or .cnf.xml corresponding to the phone device name	Name of the configuration file.	None. This message indicates the na for the phone.

Related Topics

Cisco Unified Communications Manager Documentation, on page xv

Display Network Information Screen

Use the information displayed on the Network Info screen to resolve connection issues on a phone.

A message is displayed on the phone if a user has trouble connecting to a phone network.

Procedure

Step 1 To display the Status menu, press **Applications** .

Step 2 Select **Admin settings** > **Status** > **Status messages**.

Step 3 Select **Network Info**.

Step 4 To exit Network Info, press **Exit**.

Display Network Statistics Window

To display the Network Statistics screen, perform these steps:

Procedure

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

Network Statistics Fields

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

Table 34: Network Statistics Fields

Item	Description
Tx Frames	Number of packets sent by the phone
Tx broadcast	Number of broadcast packets sent by the phone
Tx unicast	Total number of unicast packets transmitted by the phone
Rx Frames	Number of packets received by the phone
Rx broadcast	Number of broadcast packets received by the phone
Rx unicast	Total number of unicast packets received by the phone
CDP Neighbor Device ID	Identifier of a device connected to this port discovered by CDP protocol.
CDP Neighbor IP Address	Identifier of a device connected to this port discovered by CDP protocol using IP.
CDP Neighbor IPv6 Address	Identifier of a device connected to this port discovered by CDP protocol using IPv6.
CDP Neighbor Port	Identifier of a device connected to this port discovered by CDP protocol.

Item	Description
Restart Cause: One of these values: • Hardware Reset (Power-on reset) • Software Reset (memory controller also reset) • Software Reset (memory controller not reset) • Watchdog Reset • Unknown	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: • CDP BOUND • CDP INIT • DHCP BOUND • DHCP DISABLED • DHCP INIT • DHCP INVALID • DHCP REBINDING • DHCP REBOOT • DHCP RENEWING • DHCP REQUESTING • DHCP RESYNC • DHCP UNRECOGNIZED • DHCP WAITING COLDBOOT TIMEOUT • DISABLED DUPLICATE IP • SET DHCP COLDBOOT • SET DHCP DISABLED • SET DHCP FAST

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

Display Call Statistics Window

You can access the **Call statistics** menu 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 **Settings** softkey.

Step 2 Select **Admin Settings** > **Status** > **Call Statistics**.

Step 3 To exit the Status menu, press **Back**.

Call Statistics Fields

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

Table 35: Call Statistics Items for the Cisco IP Phone

Item	Description
Receiver Codec	Type of received voice stream (RTP streaming audio from codec): • G.729 • G.722 • G722.2 AMR-WB • G.711 mu-law • G.711 A-law • OPUS • iLBC

Item	Description
Sender Codec	Type of transmitted voice stream (RTP streaming audio from codec): • G.729 • G.722 • G722.2 AMR-WB • G.711 mu-law • G.711 A-law • OPUS • iLBC
Receiver Size	Size of voice packets, in milliseconds, in the receiving voice stream (RTP streaming audio).
Sender Size	Size of voice packets, in milliseconds, in the transmitting voice stream.
Rcvr Packets	Number of RTP voice packets that were received since voice stream opened. **Note** This number is not necessarily identical to the number of RTP voice packets that were received since the call began because the call might have been placed on hold.
Sender Packets	Number of RTP voice packets that were transmitted since voice stream opened. **Note** This number is not necessarily identical to the number of RTP voice packets that were transmitted since the call began because the call might have been placed on hold.
Avg Jitter	Estimated average RTP packet jitter (dynamic delay that a packet encounters when going through the network), in milliseconds, that was observed since the receiving voice stream opened.
Max Jitter	Maximum jitter, in milliseconds, that was observed since the receiving voice stream opened.
Receiver Discarded	Number of RTP packets in the receiving voice stream that were discarded (bad packets, too late, and so on). **Note** The phone discards payload type 19 comfort noise packets that Cisco Gateways generate, because they increment this counter.
Rcvr Lost Packets	Missing RTP packets (lost in transit).
Voice-Quality Metrics	

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

Display Security Setup Window

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

Procedure

Step 1 Press **Applications** .

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

Step 3 To exit, press **Back** .

Security Setup Fields

The Security Setup screen displays these items.

Table 36: Security Setup 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 secu
Trust List	The Trust List is a top-level menu that provides submenus for the C
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: Displays network setup information and information about other phone settings.
- Network Statistics: Displays hyperlinks that provide information about network traffic.
- Device Logs: Displays hyperlinks that provide information that you can use for troubleshooting.
- Streaming Statistic: Displays hyperlinks to a variety of streaming statistics.

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

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

Access the Phone Web Page

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

Procedure

Step 1 Obtain the IP address of the Cisco IP Phone by using one of these methods:

a) Search for the phone in Cisco Unified Communications Manager Administration by choosing **Device** > **Phone**. Phones that register with Cisco Unified Communications Manager display the IP address on the Find and List Phones window and at the top of the Phone Configuration window.

b) On the phone, press **Applications** and select **Admin Settings** > **Network Setup** > **IPv4 Setup**, and then scroll to the IP Address field.

Step 2 Open a web browser and enter the following URL, where *IP_address* is the IP address of the Cisco IP Phone:

http://<IP_address>

Device Information

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, and then click the **Device Information** hyperlink.

Table 37: Device Information Area Items

Item	Description
Service mode	The service mode for the phone.
Service domain	The domain for the service.
Service state	The current state of the service.
MAC Address	Media Access Control (MAC) address of the phone.
Host Name	Unique, fixed name that is automatically assigned to the phone based on the MAC address.
Phone DN	Directory number that is assigned to the phone.
App Load ID	Identifies the application load version.
Boot Load ID	Indicates the boot load version.
Version	Identifier of the firmware that is running on the phone.
Hardware Revision	Minor revision value of the phone hardware.
Serial Number	Unique serial number of the phone.
Model Number	Model number of the phone.
Message Waiting	Indicates whether is a voice message is waiting on the primary line for this phone.
UDI	Displays the following Cisco Unique Device Identifier (UDI) information about the phone: • Device Type: Indicates hardware type. For example, phone displays for all phone models. • Device Description: Displays the name of the phone associated with the indicated model type. • Product Identifier: Specifies the phone model. • Version ID (VID): Specifies the major hardware version number. • Serial Number: Displays the unique serial number of the phone.

Item	Description
Headset name	Displays the name of the attached Cisco headset in the left column. The right column contains this information: • Port—Displays how the headset connects to the phone. • Version—Displays the headset firmware version. • Radio range—Displays the strength configured for the DECT radio. Applicable to the Cisco Headset 560 Series only. • Bandwidth—Displays if the headset uses Wide band or Narrow band. Applicable to the Cisco Headset 560 Series only. • Bluetooth—Displays if Bluetooth is enabled or disabled. Applicable to the Cisco Headset 560 Series only. • Conference—Displays if the conference feature is enabled or disabled. Applicable to the Cisco Headset 560 Series only. •
Time	Time for the Date/Time Group to which the phone belongs. This information comes from Cisco Unified Communications Manager.
Time Zone	Time zone for the Date/Time Group to which the phone belongs. This information comes from Cisco Unified Communications Manager.
Date	Date for the Date/Time Group to which the phone belongs. This information comes from Cisco Unified Communications Manager.
System Free Memory	Amount of available system memory.
Java Heap Free Memory	Amount of free memory for the Java heap.
Java Pool Free Memory	Amount of free memory for the Java pool.
FIPS Mode Enabled	Indicates if the Federal Information processing Standard (FIPS) Mode is enabled.

Network Setup

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 38: Network Setup Area Items

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

Item	Description
Unified CM 1-5	Host names or IP addresses, in prioritized order, of the Cisco Unified Communications Manage with which the phone can register. An item can also show the IP address of an SRST router t capable of providing limited Cisco Unified Communications Manager functionality, if such a available. For an available server, an item shows the Cisco Unified Communications Manager server IP and one of the following states: • Active: Cisco Unified Communications Manager server from which the phone is currently r call-processing services • Standby: Cisco Unified Communications Manager server to which the phone switches if th server becomes unavailable • Blank: No current connection to this Cisco Unified Communications Manager server An item may also include the Survivable Remote Site Telephony (SRST) designation, which i an SRST router capable of providing Cisco Unified Communications Manager functionality limited feature set. This router assumes control of call processing if all other Cisco Unified Communications Manager servers become unreachable. The SRST Cisco Unified Communic Manager always appears last in the list of servers, even if it is active. You configure the SRS address in the Device Pool section in Cisco Unified Communications Manager Configuration
Information URL	URL of the help text that appears on the phone.
Directories URL	URL of the server from which the phone obtains directory information.
Messages URL	URL of the server from which the phone obtains message services.
Services URL	URL of the server from which the phone obtains Cisco IP Phone services.
Idle URL	URL that the phone displays when the phone is idle for the time that the Idle URL Time field 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 t URL specifies activates.
Proxy Server URL	URL of proxy server, which makes HTTP requests to nonlocal host addresses on behalf of th HTTP client and provides responses from the nonlocal host to the phone HTTP client.
Authentication URL	URL that the phone uses to validate requests that are made to the phone web server.
SW Port Setup	Speed and duplex of the switch port, where: • A = Auto Negotiate • 10H = 10-BaseT/half duplex • 10F = 10-BaseT/full duplex • 100H = 100-BaseT/half duplex • 100F = 100-BaseT/full duplex • 1000F = 1000-BaseT/full duplex • No Link= No connection to the switch port

Item	Description
PC Port Setup	Speed and duplex of the switch port, where: • A = Auto Negotiate • 10H = 10-BaseT/half duplex • 10F = 10-BaseT/full duplex • 100H = 100-BaseT/half duplex • 100F = 100-BaseT/full duplex • 1000F = 1000-BaseT/full duplex • No Link = No connection to the PC port
PC Port Disabled	Indicates whether the PC port on the phone is enabled or disabled.
User Locale	User locale that associates with the phone user. Identifies a set of detailed information to su including language, font, date and time formatting, and alphanumeric keyboard text infor
Network Locale	Network locale that associates with the phone user. Identifies a set of detailed information the phone in a specific location, including definitions of the tones and cadences that the p
User Locale Version	Version of the user locale that is loaded on the phone.
Network Locale Version	Version of the network locale that is loaded on the phone.
Speaker Enabled	Indicates whether the speakerphone is enabled on the phone.
Group Listen	Indicates whether the group listen feature is enabled on the phone. Group listen enables y using the handset and listen on the speaker at the same time.
GARP Enabled	Indicates whether the phone learns MAC addresses from Gratuitous ARP responses.
Span to PC Port	Indicates whether the phone forwards packets that are transmitted and received on the net the access port.
Video Capability Enabled	Indicates whether the phone can participate in video calls when it connects to an appropriat camera.
Voice VLAN Enabled	Indicates whether the phone allows a device that is attached to the PC port to access the V
PC VLAN	VLAN that identifies and removes 802.1P/Q tags from packets that are sent to the PC.
Auto Line Select Enabled	Indicates whether the phone shifts the call focus to incoming calls on all lines.
DSCP for Call Control	DSCP IP classification for call control signaling.
DSCP for Configuration	DSCP IP classification for any phone configuration transfer.
DSCP for Services	DSCP IP classification for phone-based services.
Security Mode	Security mode that is set for the phone.
Web Access Enabled	Indicates whether web access is enabled (Yes) or disabled (No) for the phone.
SSH Access Enabled	Indicates whether the phone accepts or blocks the SSH connections.

Item	Description
CDP: SW Port	Indicates whether CDP support exists on the switch port (default is enabled). Enable CDP on the switch port for VLAN assignment for the phone, power negotiation, QoS management, and 802.1x security. Enable CDP on the switch port when the phone connects to a Cisco switch. When CDP is disabled in Cisco Unified Communications Manager, a warning is presented, in that CDP should be disabled on the switch port only if the phone connects to a non-Cisco sw The current PC and switch port CDP values are shown on the Settings menu.
CDP: PC Port	Indicates whether CDP is supported on the PC port (default is enabled). When CDP is disabled in Cisco Unified Communications Manager, a warning is displays to 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.
LLDP-MED: SW Port	Indicates whether Link Layer Discovery Protocol Media Endpoint Discovery (LLDP-MED) is on the switch port.
LLDP: PC Port	Indicates whether Link Layer Discovery Protocol (LLDP) is enabled on the PC port.
LLDP Power Priority	Advertises the phone power priority to the switch, thus enabling the switch to appropriately p power to the phones. Settings include: • Unknown: This is the default value. • Low • High • Critical
LLDP Asset ID	Identifies the asset ID that is assigned to the phone for inventory management.
CTL File	Identifies the CTL file.
ITL File	The ITL file contains the initial trust list.
ITL Signature	Enhances security by using the secure hash algorithm (SHA-1) in the CTL and ITL files.
CAPF Server	The name of the CAPF server used by the phone.
TVS	The main component of Security by Default. Trust Verification Services (TVS) enables Cisco IP Phones to authenticate application servers, such as EM services, directory, and MIDlet, du HTTPS establishment.
TFTP Server	The name of the TFTP Server used by the phone.
TFTP Server	The name of the TFTP Server used by the phone.
Automatic Port Synchronization	Synchronizes the ports to the lower speed which eliminates packet loss.
Switch Port Remote Configuration	Allows the administrator to configure the speed and function of the Cisco Desktop Collabora Experience table port remotely by using Cisco Unified Communications Manager Administr

Item	Description
PC Port Remote Configuration	Indicates if remote port configuration of the speed and duplex mode for the PC port is ena disabled.
IP Addressing Mode	Displays the IP addressing mode that is available on the phone.
IP Preference Mode Control	Indicates the IP address version that the phone uses during signaling with Cisco Unified Com Manager when both IPv4 and IPv6 are both available on the phone.
IP Preference Mode For Media	Indicates that for media the device uses an IPv4 address to connect to the Cisco Unified Com Manager.
IPv6 Auto Configuration	Displays whether the auto configuration is enabled or disabled on the phone.
IPv6 DAD	Verifies the uniqueness of new unicast IPv6 addresses before the addresses are assigned t
IPv6 Accept Redirect Message	Indicates if phone accepts the redirect messages from the same router that is used for the number.
IPv6 Reply Multicast Echo Request	Indicates that the phone sends an Echo Reply message in response to an Echo Request m to an IPv6 address.
IPv6 Load Server	Used to optimize installation time for phone firmware upgrades and off load the WAN by images locally, negating the need to traverse the WAN link for each phone's upgrade.
IPv6 Log Server	Indicates the IPv6-only address and port of the remote logging machine to which the pho messages.
IPv6 CAPF Server	Common Name (from the Cisco Unified Communications Manager Certificate) of the CA the phone.
DHCPv6	Dynamic Host Configuration Protocol (DHCP) automatically assigns IPv6 address to dev you connect them to the network. Cisco Unified IP Phones enable DHCP by default.
IPv6 Address	Displays the current IPv6-only address of the phone or allows the user to enter a new IPv
IPv6 Prefix Length	Displays the current prefix length for the subnet or allows the user to enter a new prefix l
IPv6 Default Router 1	Displays the default router used by the phone or allows the user to enter a new IPv6 defau
IPv6 DNS Server 1	Displays the primary DNSv6 server used by the phone or allows the user to enter a new s
IPv6 DNS Server 2	Displays the secondary DNSv6 server used by the phone or allows the user to set a new s DNSv6 server.
IPv6 Alternate TFTP	Allows the user to enable the use of an alternate (secondary) IPv6 TFTP server.
IPv6 TFTP Server 1	Displays the primary IPv6 TFTP server used by the phone or allows the user to set a new pr server.
IPv6 TFTP Server 2	Displays the secondary IPv6 TFTP server used if the primary IPv6 TFTP server is unavailal the user to set a new secondary TFTP server.
IPv6 Address Released	Allows the user to release IPv6-related information.

Item	Description
Energywise Power Level	A measure of the energy consumed by devices in an EnergyWise network. The Cisco IP Phone 7811 does not support Energywise Power Level.
Energywise Domain	An administrative grouping of devices for the purpose of power monitoring and control. The Cisco IP Phone 7811 does not support Energywise Domain.

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

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 176

Ethernet Information Web Page

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

Table 39: Ethernet Information Items

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

Access Area and Network Area Web Pages

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

Table 40: 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.
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.

Item	Description
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.
CDP Neighbor IPv6 Address	IPv6 address of the neighbor device discovered that CDP protocol discovered.
CDP Neighbor Port	Neighbor device port to which the phone is connected discovered by CDP protocol.
LLDP Neighbor Device ID	Identifier of a device connected to this port discovered by LLDP discovered.
LLDP Neighbor IP Address	IP address of the neighbor device that LLDP protocol discovered.
LLDP Neighbor IPv6 Address	IPv6 address of the neighbor device discovered that CDP 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.

- 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 Window 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 41: Streaming Statistics area items

Item	Description
Remote Address	IP address and UDP port of the destination of the stream.
Local Address	IP address and UPD port of the phone.
Start Time	Internal time stamp indicates when Cisco Unified Communications Manager request 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 a
Sender Packets	Total number of RTP data packets that the phone transmitted since it started this co 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 sinc this connection. The value is 0 if the connection is set to receive-only mode.
Sender Codec	Type of audio encoding that is for the transmitted stream.
Sender Reports Sent (see note)	Number of times the RTCP Sender Report has been sent.

Item	Description
Sender Report Time Sent (see note)	Internal time-stamp indication as to when the last RTCP Sender Report was sent.
Rcvr Lost Packets	Total number of RTP data packets that have been lost since data reception started on th connection. Defined as the number of expected packets less the number of packets actu received, where the number of received packets includes any that are late or are duplicat 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 millise The value displays as 0 if the connection was set to send-only mode.
Receiver Codec	Type of audio encoding that is used for the received stream.
Receiver Reports Sent (see note)	Number of times the RTCP Receiver Reports have been sent.
Receiver Report Time Sent (see note)	Internal time-stamp indication as to when a RTCP Receiver Report was sent.
Rcvr Packets	Total number of RTP data packets that the phone has received since data reception start this connection. Includes packets that were received from different sources if this call i multicast call. The value displays as 0 if the connection was set to send-only mode.
Rcvr Octets	Total number of payload octets that the device received in RTP data packets since recep started on the connection. Includes packets that were received from different sources if t 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 re from the start of the voice stream.
Interval Conceal Ratio	Ratio of concealment frames to speech frames in the preceding 3-second interval of act speech. If voice activity detection (VAD) is in use, a longer interval might be required t accumulate three seconds of active speech.
Max Conceal Ratio	Highest interval concealment ratio from the start of the voice stream.
Conceal Seconds	Number of seconds that have concealment events (lost frames) from the start of the voice (includes severely concealed seconds).
Severely Conceal Seconds	Number of seconds that have more than five percent concealment events (lost frames) fr start of the voice stream.
Latency (see note)	Estimate of the network latency, expressed in milliseconds. Represents a running avera the round-trip delay, measured when RTCP receiver report blocks are received.
Max Jitter	Maximum value of instantaneous jitter, in milliseconds.
Sender Size	RTP packet size, in milliseconds, for the transmitted stream.

Item	Description
Sender Reports Received (see note)	Number of times RTCP Sender Reports have been received.
Sender Report Time Received (see note)	Most recent time when an RTCP Sender Report was received.
Receiver Size	RTP packet size, in milliseconds, for the received stream.
Receiver Discarded	RTP packets that were received from the network but were discarded from the jitter
Receiver Reports Received (see note)	Number of times RTCP Receiver Reports have been received.
Receiver Report Time Received (see note)	Most recent time when an RTCP Receiver Report was received.

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

Request Information from the Phone in XML

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

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

Before you begin

Web access needs to be enabled to get the information.

The phone must be associated with a user.

Procedure

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

where

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

The command returns an XML document.

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

where

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

The command returns an XML document.

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

where

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

The command returns an XML document.

Sample CallInfo Output

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

```
<?xml version="1.0" encoding="UTF-8"?>
<CiscoIPPhoneCallLineInfo>
  <Prompt/>
  <Notify/>
  <Status/>
  <LineDirNum>1030</LineDirNum>
  <LineState>CONNECTED</LineState>
  <CiscoIPPhoneCallInfo>
     <CallState>CONNECTED</CallState>
     <CallType>INBOUND</CallType>
     <CallingPartyName/>
     <CallingPartyDirNum>9700</CallingPartyDirNum>
     <CalledPartyName/>
     <CalledPartyDirNum>1030</CalledPartyDirNum>
     <HuntPilotName/>
     <CallReference>30303060</CallReference>
     <CallDuration>12835</CallDuration>
     <CallStatus>null</CallStatus>
     <CallSecurity>UNAUTHENTICATED</CallSecurity>
     <CallPrecedence>ROUTINE</CallPrecedence>
     <FeatureList/>
   </CiscoIPPhoneCallInfo>
   <VisibleFeatureList>
     <Feature Position="1" Enabled="true" Label="End Call"/>
     <Feature Position="2" Enabled="true" Label="Show Detail"/>
   </VisibleFeatureList>
</CiscoIPPhoneCallLineInfo>
```

Sample LineInfo Output

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

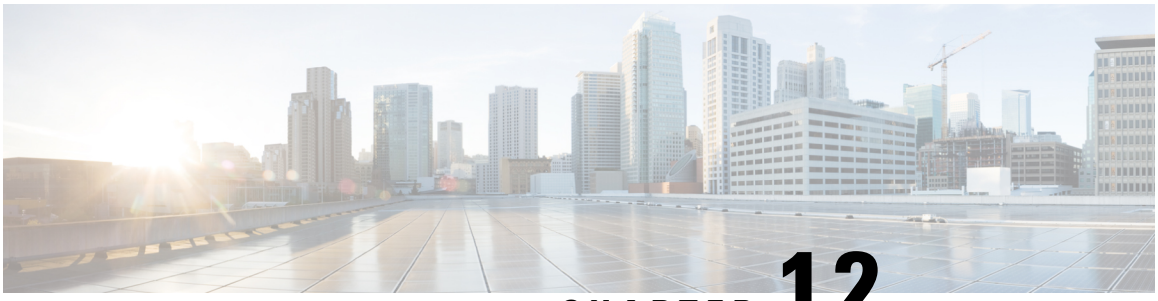
```
<CiscoIPPhoneLineInfo>
   <Prompt/>
   <Notify/>
   <Status>null</Status>
   <CiscoIPPhoneLines>
     <LineType>9</LineType>
     <lineDirNum>1028</lineDirNum>
     <MessageWaiting>NO</MessageWaiting>
     <RingerName>Chirp1</RingerName>
     <LineLabel/>
     <LineIconState>ONHOOK</LineIconState>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

Sample ModeInfo Output

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

```
<?xml version="1.0" encoding="utf-8"?>
<CiscoIPPhoneModeInfo>
   <PlaneTitle>Applications</PlaneTitle>
   <PlaneFieldCount>12</PlaneFieldCount>
   <PlaneSoftKeyIndex>0</PlaneSoftKeyIndex>
   <PlaneSoftKeyMask>0</PlaneSoftKeyMask>
   <Prompt></Prompt>
   <Notify></Notify>
   <Status></Status>
   <CiscoIPPhoneFields>
      <FieldType>0</FieldType>
      <FieldAttr></FieldAttr>
      <fieldHelpIndex>0</fieldHelpIndex>
      <FieldName>Call History</FieldName>
      <FieldValue></FieldValue>
   </CiscoIPPhoneFields>
   <CiscoIPPhoneFields>
      <FieldType>0</FieldType>
      <FieldAttr></FieldAttr>
      <fieldHelpIndex>0</fieldHelpIndex>
      <FieldName>Preferences</FieldName>
      <FieldValue></FieldValue>
```

```
    </CiscoIPPhoneFields>
    ...
</CiscoIPPhoneModeInfo>
```



CHAPTER 12

Troubleshooting

- General Troubleshooting Information, on page 193
- Startup Problems, on page 194
- Phone Reset Problems, on page 198
- Phone Cannot Connect to LAN, on page 200
- Cisco IP Phone Security Problems, on page 201
- Audio Problems, on page 203
- Troubleshooting Procedures, on page 203
- Control Debug Information from Cisco Unified Communications Manager, on page 208
- Additional Troubleshooting Information, on page 209

General Troubleshooting Information

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

Table 42: 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 thr port. Each IP Phone should connect directly to a switch port. If phones a together in a line by using the PC port, the phones do not work. **Note** The Cisco 7832 conference phone does not have a PC port.
Prolonged broadcast storms cause IP phones to reset, or be unable to make or answer a call	A prolonged Layer 2 broadcast storm (lasting several minutes) on the v may cause IP phones to reset, lose an active call, or be unable to initiat call. Phones may not come up until a broadcast storm ends.

Summary	Explanation
Moving a network connection from the phone to a workstation	If you power your phone through the network connection, you must be care decide to unplug the network connection of the phone and plug the cable into computer. **Caution** The network card in the computer cannot receive power through the netwo connection; if power comes through the connection, the network card can destroyed. To protect a network card, wait 10 seconds or longer after unplu the cable from the phone before plugging it into a computer. This delay giv switch enough time to recognize that there is no longer a phone on the line stop providing power to the cable.
Changing the telephone configuration	By default, the administrator password settings are locked to prevent users making changes that could impact their network connectivity. You must un administrator password settings before you can configure them. See Apply a Phone Password, on page 44 for details. **Note** If the administrator password is not set in common phone profile, then use modify the network settings.
Codec mismatch between the phone and another device	The RxType and the TxType statistics show the codec that is used for a con between this Cisco IP Phone and the other device. The values of these statisti match. If they do not, verify that the other device can handle the codec conv or that a transcoder is in place to handle the service. See Display Call Stati Window, on page 173 for details.
Sound sample mismatch between the phone and another device	The RxSize and the TxSize statistics show the size of the voice packets tha in a conversation between this Cisco IP Phone and the other device. The va these statistics should match. See Display Call Statistics Window, on page details.
Loopback condition	A loopback condition can occur when the following conditions are met: • The SW Port Configuration option on the phone is set to 10 Half (10-B duplex). • The phone receives power from an external power supply. • The phone is powered down (the power supply is disconnected). In this case, the switch port on the phone can become disabled and the foll message appears in the switch console log: HALF_DUX_COLLISION_EXCEED_THRESHOLD To resolve this problem, reenable the port from the switch.

Startup Problems

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

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

Related Topics

Verify Phone Startup, on page 51

Cisco IP Phone Does Not Go Through the Normal Startup Process

Problem

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

Cause

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

Solution

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

- Verify that the network port is functional:
  - Exchange the Ethernet cables with cables that you know are functional.
  - Disconnect a functioning Cisco IP Phone from another port and connect it to this network port to verify that the port is active.
  - Connect the Cisco IP Phone that does not start up to a different network port that is known to be good.
  - Connect the Cisco IP Phone that does not start up directly to the port on the switch, eliminating the patch panel connection in the office.
- Verify that the phone is receiving power:
  - If you are using external power, verify that the electrical outlet is functional.
  - If you are using in-line power, use the external power supply instead.
  - If you are using the external power supply, switch with a unit that you know to be functional.
- If the phone still does not start up properly, power up the phone by pressing #*2. 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 51

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 203 for more information.

Phone Displays Error Messages

Problem

Status messages display errors during startup.

Solution

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

Related Topics

Display Status Messages Window, on page 164

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 204

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 205

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 207

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 207.

Configuration File Corruption

Problem

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

Solution

Create a new phone configuration file.

Cisco Unified Communications Manager Phone Registration

Problem

The phone is not registered with the Cisco Unified Communications Manager

Solution

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

To verify that the phone is in the Cisco Unified Communications Manager database, choose **Device** > **Phone** from Cisco Unified Communications Manager Administration. Click **Find** to search for the phone based on the MAC Address. For information about determining a MAC address, see Determine the Phone MAC Address, on page 60.

If the phone is already in the Cisco Unified Communications Manager database, the configuration file may be damaged. See Configuration File Corruption, on page 197 for assistance.

Cisco IP Phone Cannot Obtain IP Address

Problem

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

Solution

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

Phone Reset Problems

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

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

Phone Resets Due to Intermittent Network Outages

Problem

Your network may be experiencing intermittent outages.

Solution

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

Phone Resets Due to DHCP Setting Errors

Problem

The DHCP settings may be incorrect.

Solution

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

Related Topics

Check DHCP Settings, on page 205

Phone Resets Due to Incorrect Static IP Address

Problem

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

Solution

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

Phone Resets During Heavy Network Usage

Problem

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

Solution

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

Phone Resets Due to Intentional Reset

Problem

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

Solution

You can check if a Cisco IP Phone received a command from Cisco Unified Communications Manager to reset by pressing **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 205.

Phone Does Not Power Up

Problem

The phone does not appear to be powered up.

Solution

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

Phone Cannot Connect to LAN

Problem

The physical connection to the LAN may be broken.

Solution

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

Cisco IP Phone Security Problems

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

CTL File Problems

The following sections describe troubleshooting problems with the CTL file.

Authentication Error, Phone Cannot Authenticate CTL File

Problem

A device authentication error occurs.

Cause

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

Solution

Install a correct certificate.

Phone Cannot Authenticate CTL File

Problem

Phone cannot authenticate the CTL file.

Cause

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

Solution

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

CTL File Authenticates but Other Configuration Files Do Not Authenticate

Problem

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

Cause

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

Solution

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

ITL File Authenticates but Other Configuration Files Do Not Authenticate

Problem

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

Cause

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

Solution

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

TFTP Authorization Fails

Problem

Phone reports TFTP authorization failure.

Cause

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

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

Solution

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

Phone Does Not Register

Problem

Phone does not register with Cisco Unified Communications Manager.

Cause

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

Solution

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

Signed Configuration Files Are Not Requested

Problem

Phone does not request signed configuration files.

Cause

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

Solution

Configure TFTP entries with certificates in the CTL file.

Audio Problems

The following sections describe how to resolve audio problems.

No Speech Path

Problem

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

Solution

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

Choppy Speech

Problem

A user complains of choppy speech on a call.

Cause

There may be a mismatch in the jitter configuration.

Solution

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

Troubleshooting Procedures

These procedures can be used to identify and correct problems.

Create a Phone Problem Report from Cisco Unified Communications Manager

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

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

Procedure

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

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

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

Create a Console Log from Your Phone

You generate a console log when your phone will not connect to the network and you cannot access the Problem Report Tool (PRT).

Before you begin

Connect a console cable to the Auxiliary port on the back of your phone.

Procedure

Step 1 On your phone, press **Applications** .

Step 2 Navigate **Admin settings** > **Aux port**.

Step 3 Select **Collect console log** to collect device logs.

Check TFTP Settings

Procedure

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

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

Step 3 Check the TFTP Server 1 field.

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

If you are using DHCP, the phone obtains the address for the TFTP server from the DHCP server. Check that the IP address is configured in Option 150.

Step 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 scenarios.

Related Topics

Phone Cannot Connect to TFTP Server, on page 196

Determine DNS or Connectivity Issues

Procedure

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

Step 2 Modify DHCP and IP settings:

a) Disable DHCP.

b) Assign static IP values to the phone. Use the same default router setting that other functioning phones use.

c) Assign a TFTP server. Use the same TFTP server that other functioning phones use.

Step 3 On the Cisco Unified Communications Manager server, verify that the local host files have the correct Cisco Unified Communications Manager server name mapped to the correct IP address.

Step 4 From Cisco Unified Communications Manager, choose **System** > **Server** and verify that reference to the server is made by the IP address and not by the DNS name.

Step 5 From Cisco Unified Communications Manager, choose **Device** > **Phone**. Click **Find** to search for this phone. Verify that you have assigned the correct MAC address to this Cisco IP Phone.

Step 6 Power cycle the phone.

Related Topics

Basic Reset, on page 211
Determine the Phone MAC Address, on page 60

Check DHCP Settings

Procedure

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

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

Step 3 Check the DHCP server field.

If you have assigned a static IP address to the phone, you do not need to enter a value for the DHCP Server option. However, if you are using a DHCP server, this option must have a value. If no value is found, check

your IP routing and VLAN configuration. See the *Troubleshooting Switch Port and Interface Problems* document, available at this URL:

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

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

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

Step 5 If you are using DHCP, check the IP addresses that your DHCP server distributes.

See the *Understanding and Troubleshooting DHCP in Catalyst Switch or Enterprise Networks* document, available at this URL:

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

Related Topics

Phone Cannot Connect to Server, on page 197
Phone Resets Due to DHCP Setting Errors, on page 199

Create a New Phone Configuration File

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

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

Procedure

Step 1 From Cisco Unified Communications Manager, choose **Device** > **Phone** and click **Find** to locate the phone that is experiencing problems.

Step 2 Choose **Delete** to remove the phone from the Cisco Unified Communications Manager database.

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

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

Step 4 Power cycle the phone.

Related Topics

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

Verify DNS Settings

Procedure

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

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

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

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

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

Related Topics

Phone Cannot Connect Using DNS, on page 197

Start Service

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

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Cisco Unified Serviceability** from the Navigation drop-down list and click **Go**.

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

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

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

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

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

Control Debug Information from Cisco Unified Communications Manager

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

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

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

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

Contact Cisco TAC for more information and assistance.

Procedure

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

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

Step 2 Set the following parameters:

- Log Profile - values: Preset (default), Default, Telephony, SIP, UI, Network, Media, Upgrade, Accessory, Security, Wi-Fi, VPN, Energywise, MobileRemoteAccess

  Note
  To implement multilevel and multi-section support of the parameters, check the Log Profile check box.

- Remote Log - values: Disable (default), Enable
- IPv6 Log Server or Log Server - IP address (IPv4 or IPv6 address)

Note

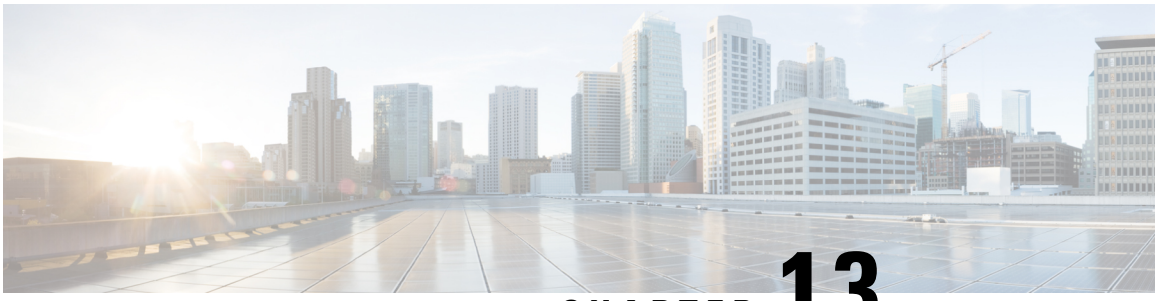
When the Log Server cannot be reached, the phone stops sending debug messages.

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

Additional Troubleshooting Information

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

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



CHAPTER 13

Maintenance

- Basic Reset, on page 211
- Remove CTL File, on page 213
- Voice Quality Monitoring, on page 214
- Cisco IP Phone Cleaning, on page 215

Basic Reset

Performing a basic reset of a Cisco IP Phone provides a way to recover when the phone experiences an error. The reset 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 applicable for your situation.

Table 43: Basic Reset Methods

Operation	Action	Expla
Restart phone	Press **Services**, **Applications**, or **Directories** and then press ****#****. Press **Settings** and choose **Device Administration** > **Restart**.	Reset writte
Reset settings	Press **Settings** and choose **Device Administration** > **Factory Reset**.	Resto
	To reset settings, press **Applications** > **Admin Settings** > **Custom Reset**.	Resto

Related Topics

Determine DNS or Connectivity Issues, on page 205

Factory Reset the Phone with the Keypad

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

Before you begin

You must know if your phone is an original hardware release or if the hardware has been updated and re-released.

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 On earlier hardware versions, the Mute button lights up. Wait for the Mute button to turn off.

Related Topics

Hardware Versions, on page 25

Perform Reset All Settings 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.

Perform Factory Reset from Phone Menu

Procedure

Step 1 Press **Applications** .

Step 2 Select **Device administration** > **Factory reset**.

Step 3 Scroll to **Admin Settings** > **Reset Settings**, and select **All**.

Step 4 To restore phone configuration or settings to factory default, press **OK**.

Perform Custom Reset from Phone Menu

Procedure

Step 1 Press **Applications** .

Step 2 Scroll to **Admin Settings** and select **Custom Reset**.

Step 3 To restore phone configuration or settings to noncustomized default, press **Ok**.

Reboot Your Phone from the Backup Image

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

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

Procedure

Step 1 Disconnect the power supply.

Step 2 Press and hold the pound (#) key.

Step 3 Reconnect the power. Continue pressing the pound key until the **Speakerphone** and **Headset** buttons turn green.

Step 4 Release the pound key.

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** .

Voice Quality Monitoring

To measure the voice quality of calls that are sent and received within the network, Cisco IP Phones use these statistical metrics that are based on concealment events. The DSP plays concealment frames to mask frame loss in the voice packet stream.

- Concealment Ratio metrics—Show the ratio of concealment frames over total speech frames. An interval conceal ratio is calculated every 3 seconds.
- Concealed Second metrics—Show the number of seconds in which the DSP plays concealment frames due to lost frames. A severely "concealed second" is a second in which the DSP plays more than five percent concealment frames.

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

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

Voice Quality Troubleshooting Tips

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

Table 44: Changes to Voice Quality Metrics

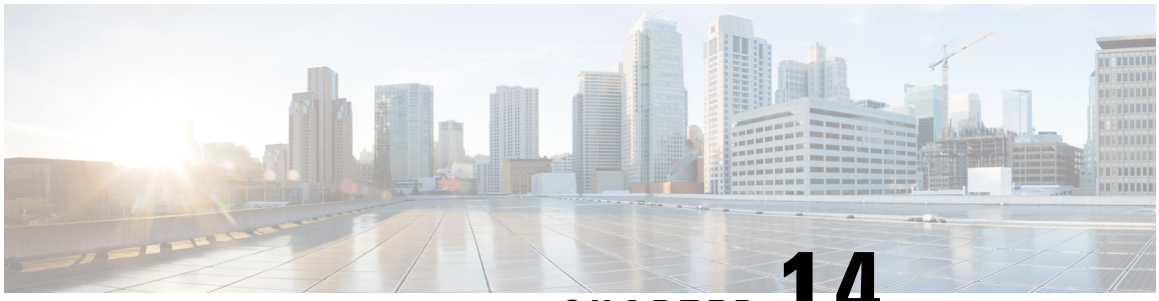
Metric Change	Condition
Conceal Ratio and Conceal Seconds increase significantly	Network impairment from packet loss or high jitter.
Conceal Ratio is near or at zero, but the voice quality is poor.	• Noise or distortion in the audio channel such as echo or audio levels. • Tandem calls that undergo multiple encode/decode such as calls to a cellular network or calling card network. • Acoustic problems coming from a speakerphone, handsfree cellular phone or wireless headset. Check packet transmit (TxCnt) and packet receive (RxCnt) counters to verify that voice packets are flowing.

Note Voice quality metrics do not account for noise or distortion, only frame loss.

Cisco IP Phone Cleaning

To clean your Cisco IP Phone, use only a dry soft cloth to gently wipe the phone and the phone screen. Do not apply liquids or powders directly to the phone. As with all non-weatherproof electronics, liquids and powders can damage the components and cause failures.

When the phone is in sleep mode, the screen is blank and the Select button is not lit. When the phone is in this condition, you can clean the screen, as long as you know that the phone will remain asleep until after you finish cleaning.



CHAPTER 14

International User Support

- Unified Communications Manager Endpoints Locale Installer, on page 217
- International Call Logging Support, on page 217
- Language Limitation, on page 218

Unified Communications Manager Endpoints Locale Installer

By default, Cisco IP Phones are set up for the English (United States) locale. To use the Cisco IP Phones in other locales, you must install the locale-specific version of the Unified Communications Manager Endpoints Locale Installer on every Cisco Unified Communications Manager server in the cluster. The Locale Installer installs the latest translated text for the phone user interface and country-specific phone tones on your system so that they are available for the Cisco IP Phones.

To access the Locale Installer required for a release, access the Software Download page, navigate to your phone model, and select the Unified Communications Manager Endpoints Locale Installer link.

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

Note The latest Locale Installer may not be immediately available; continue to check the website for updates.

Related Topics

Cisco Unified Communications Manager Documentation, on page xv

International Call Logging Support

If your phone system is configured for international call logging (calling party normalization), the call logs, redial, or call directory entries may display a plus (+) symbol to represent the international escape code for your location. Depending on the configuration for your phone system, the + may be replaced with the correct international dialing code, or you may need to edit the number before dialing to manually replace the + with the international escape code for your location. In addition, while the call log or directory entry may display the full international number for the received call, the phone display may show the shortened local version of the number, without international or country codes.

Language Limitation

There is no localized Keyboard Alphanumeric Text Entry (KATE) support for the following Asian locales:

- Chinese (China)
- Chinese (Hong Kong)
- Chinese (Taiwan)
- Japanese (Japan)
- Korean (Korea Republic)

The default English (United States) KATE is presented to the user instead.

For example, the phone screen will show text in Korean, but the **2** key on the keypad will display **a b c 2 A B C**.